ELSEVIER

Theoretical Computer Science 186 (1997) 107–134

Theoretical Computer Science

The synthesis problem for elementary net systems is NP-complete[1]

Eric Badouel, Luca Bernardinello, Philippe Darondeau*

Irisa, Campus de Beaulieu, F-35042 Rennes cedex, France

Received August 1995; revised June 1996
Communicated by G. Rozenberg

Abstract

Given a labelled graph representing the sequential behaviour of some system, the synthesis problem consists in deciding whether it is the behaviour of a Petri net. This problem was solved by Ehrenfeucht and Rozenberg for the class of elementary net systems, relying on *regions in graphs* introduced as sets of nodes liable to represent extensions of places of a net. The solution was extended later on to pure place/transition nets using a variant notion of *generalized regions*. The naive method of synthesis which relies on this principle leads to exponential algorithms for an arbitrary class of nets. In an earlier study, we gave an algorithm that solves the synthesis problem in polynomial time for the class of pure place/transition nets. We show here that in contrast the synthesis problem is indeed NP-complete for the class of elementary nets.

1. Introduction

The synthesis problem for nets consists in deciding whether a given automaton, representing the behaviour of some system, is isomorphic to the state graph of a net, and then constructing that net. Applications may be found in the engineering of distributed protocols and of asynchronous circuits [4]. The synthesis problem was solved originally for the class of elementary net systems [8], relying on *regions in graphs* introduced as sets of nodes liable to represent extensions of places with boolean values. The solution was extended later on to (pure) place/transition nets [3, 7, 12] using the variant notion of *generalized regions in graphs*, seen as multisets of nodes representing extensions of places with values given by whole numbers. A direct computation of these sets of regions would lead to algorithms taking an exponential time for the decision of the synthesis problem. However, this upper bound is not tight for every class of nets:

* Corresponding author. E-mail: darondeau@irisa.fr.

[1] This work was partly supported by the French P.R.C. *Modèles et Preuves*, by the H.C.M. Network *Express*, and by the H.C.M. fellowship granted to Luca Bernardinello, on leave from the University of Milan.

PII S0304-3975(96)00219-8

[1] gives an algorithm that solves the synthesis problem in polynomial time for the class of pure bounded and weighted place/transition nets. For the more basic class of elementary nets, a practical synthesis algorithm is given in [5], but no complexity bound is indicated in that reference. We show in this paper that the synthesis problem is in fact NP-complete for the class of elementary nets. This result, which reinforces logically independent results by Hiraishi [11], could not be foreseen with certainty: it suffices to extend elementary nets with flow arcs interpreted as switching the values of places to bring the complexity of the synthesis problem down to polynomial time [13]. The remaining part of the paper is divided in two main sections. Section 2 gives a detailed account of the synthesis problem for elementary net systems. We show in particular that this problem amounts to solving a (polynomial) number of instances of the so-called *separation problems*, each of which takes the form of a system of clauses to be satisfied in the boolean ring $\mathbb{Z}/2\mathbb{Z}$. Section 3 addresses the issue of complexity. We show that the classical problem 3-SAT reduces via the boolean ring to the synthesis problem for elementary net systems, thus proving its NP-completeness.

2. The synthesis problem for elementary net systems

2.1. Elementary net systems

We recall here a few basic definitions needed for self containment.

Definition 1 (*C/E Net*). A condition/event net is a triple (P,E,F) where P is a set of places or conditions, E is a set of events or actions disjoint from P, and $F \subset E \times P \cup P \times E$ is a bipartite relation between places and events called the flow relation. The flow graph is assumed to have no isolated element, in the sense that

$$\forall x \in E \cup P \quad \exists y \in E \cup P \qquad [(x,y) \in F \vee (y,x) \in F]$$

In the graphical representation of nets, places are depicted by circles and actions by boxes. Since the flow relation is bipartite there is no arc between two places or between two actions. We adopt the notations ${}^\bullet x = \{y/F(y,x)\}$ and $x^\bullet = \{y/F(x,y)\}$ for the respective pre-set and post-set of an element $x \in P \cup E$.

Definition 2. A C/E net is said to be *simple* when

$$\forall x, y \in P \cup E \quad ({}^\bullet x = {}^\bullet y \text{ and } x^\bullet = y^\bullet) \Rightarrow x = y$$

A *marking* of a C/E net is a set of places representing a *state* in the evolution of the net by the set of conditions it satisfies. All the possible evolutions are described in a transition system $(\mathscr{M},E,T)$ whose set of states is the set $\mathscr{M}$ of markings, and whose transitions are given by

$$M \xrightarrow{e} M' \quad \text{iff} \quad {}^\bullet e \subseteq M \quad \text{and} \quad (M \setminus {}^\bullet e) \cap e^\bullet = \emptyset \quad \text{and} \quad M' = (M \setminus {}^\bullet e) \cup e^\bullet$$

Places in ${}^\bullet e \cap e^\bullet$, called the *side conditions*[2] of e, are just tested upon: these conditions are necessary for firing event e and they still hold thereafter. The conditions in ${}^\bullet e$ (*preconditions* of e) which are not side conditions of e are also necessary for firing event e but they no longer hold after it has been fired. Symmetrically, the conditions in $e^\bullet$ (*postconditions* of e) which are not side conditions of e hold never in markings giving concession to event e, and hold always after e's executions. A net free from side conditions ($\forall e \in E \ {}^\bullet e \cap e^\bullet = \emptyset$) is said to be *pure*. The transition relation of pure C/E nets simplifies to

$$M \xrightarrow{e} M' \quad \text{iff} \quad {}^\bullet e \subseteq M \quad \text{and} \quad M \cap e^\bullet = \emptyset \quad \text{and} \quad M' = (M \setminus {}^\bullet e) \cup e^\bullet$$

Definition 3 (*Elementary net system*). An elementary net is a pure and simple C/E net with no isolated element. An elementary net system $\mathcal{N} = (P, E, F, M_0)$ is an elementary net together with an initial marking M_0 such that every event $e \in E$ may be fired at some marking reachable from M_0.

Definition 4 (*Transition system, automaton*). A transition system is a triple (S, E, T) where S is a set of states, E is a set of events, and $T \subseteq S \times E \times S$ is a set of (labelled) transitions. $(s, e, s') \in T$ is also denoted by $s \xrightarrow{e} s'$. An automaton (S, E, T, s_0) is a transition system with a distinguished state $s_0 \in S$, called the initial state.

Definition 5 (*State graph*). The state graph of an elementary net system $\mathcal{N} = (P, E, F, M_0)$ is the automaton $\mathcal{N}^* = (S, E, T, s_0)$ whose initial state s_0 is the initial marking M_0 of $\mathcal{N}$ and whose underlying transition system (S, E, T) is the induced restriction of the transition system generated from the net (P, E, F) on the set of markings reachable from M_0.

Observation 6. *If an automaton* $\mathscr{A} = (S, E, T, s_0)$ *is the state graph of an elementary net system, then it satisfies the following*: (i) *it has no loop*: $s \xrightarrow{a} s' \Rightarrow s \neq s'$, (ii) *it has no multiple transitions between states*: $(s \xrightarrow{e_1} s' \wedge s \xrightarrow{e_2} s') \Rightarrow e_1 = e_2$, (iii) *it is reduced*: $\forall e \in E \ \exists s \xrightarrow{e} s'$, *and* (iv) *it is reachable*: $\forall s \in S \ s_0 \xrightarrow{*} s$ *where* $\xrightarrow{*} = (\bigcup_{e \in E} \xrightarrow{e})^*$.

2.2. Regions in graphs

In this section, we introduce regions in graphs as they were defined originally by Ehrenfeucht and Rozenberg, then we show an equivalent definition of regions as morphisms of transition systems, and last we define the dual of a graph as the net synthesized from all regions in that graph, seen as places fully specified by the attached flow arcs.

Let $\mathscr{A} = (S, E, T, s_0)$ be an automaton. Solving the synthesis problem for this automaton in the context of elementary net systems consists in deciding whether there exists an elementary net system $\mathcal{N} = (P, E, F, M_0)$ with state graph $\mathcal{N}^*$ isomorphic to

[2] For some authors however there is no side condition for an event in a C/E net.

$\mathscr{A}$ (i.e. identical to $\mathscr{A}$ up to a bijective renaming of states and transitions). Suppose such an isomorphism exists between $\mathscr{A}$ and $\mathscr{N}^*$, then each state of the automaton $\mathscr{A}$ may be identified with a marking of the elementary net system $\mathscr{N}$ and a binary relation $\models \subseteq S \times P$ may be defined between states of $\mathscr{A}$ and places of $\mathscr{N}$ by setting $s \models x$ (read "s satisfies x") if and only if the condition x belongs to the marking associated with the state s. The elementary net $N = (P, E, F)$ provides a faithful *set-theoretic representation* of the transition system $\mathrm{T} = (S, E, T)$: the pair of mappings $[\![\cdot]\!]_S : S \to 2^P$ and $[\![\cdot]\!]_E : E \to 2^P \times 2^P$ defined as $[\![s]\!]_S = \{x \in P \mid s \models x\}$ (the marking associated with s) and $[\![e]\!]_E = \langle {}^\bullet e, e^\bullet \rangle$ are injective and the transition relation of T satisfies

$$s \xrightarrow{e} s' \in T \quad \text{iff} \quad [\![s]\!]_S \setminus [\![s']\!]_S = {}^\bullet e \quad \wedge \quad [\![s']\!]_S \setminus [\![s]\!]_S = e^\bullet$$

In order to construct a representation for a given transition system $\mathrm{T} = (S, E, T)$, one has to guess an adequate set of places (the atomic symbols of this representation). For that purpose one may use reverse reasoning, starting from the assumption that an adequate representation $N = (P, E, F)$ has been found. Then each condition $x \in P$ can be represented by the set $[\![x]\!]_P = \{s \in S \mid s \models x\}$ of states of T satisfying this condition. This set $[\![x]\!]_P$, called the *extension* of x, satisfies the predicate:

$$\begin{aligned} &\textbf{Region}(X) \equiv \textit{for every event } e \in E: \\ &\quad s \xrightarrow{e} s' \Rightarrow (s \in X \text{ and } s' \notin X) \\ &\textit{or}\quad s \xrightarrow{e} s' \Rightarrow (s \notin X \text{ and } s' \in X) \\ &\textit{or}\quad s \xrightarrow{e} s' \Rightarrow (s \in X \text{ iff } s' \in X) \end{aligned}$$

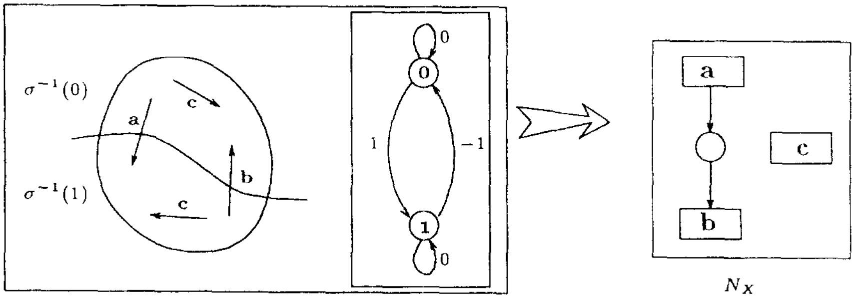
The three cases above are met respectively for $x \in {}^\bullet e$, $x \in e^\bullet$, and $x \notin {}^\bullet e \cup e^\bullet$ in $\mathscr{N}$. Now forgetting about $\mathscr{N}$, we call a *region* in T any subset $X \subseteq S$ satisfying **Region**(X).

Observation 7. *Let $\mathscr{N}$ be an elementary net system with set of places P and marking graph $\mathscr{N}^* = (S, E, T, s_0)$ – thus $S \subsetneq 2^P$. If $x \in P$ then its extension $[\![x]\!] = \{M \in S/x \in M\}$ is a region of $\mathscr{N}^*$.*

As a matter of fact, a set $X \subseteq S$ is a region if and only if its characteristic function $\sigma = \chi_X : S \to \{0, 1\}$ admits a (unique) companion map $\eta : E \to \{-1, 0, 1\}$ such that $\sigma(s') = \sigma(s) + \eta(e)$ for every transition $s \xrightarrow{e} s'$ in T. From now on, we identify regions with such pairs of mappings (σ, η) which turn to be exactly the morphisms of transitions systems[3] from $\mathrm{T} = (S, E, T)$ to the *classifying* transition system $2 = (\{0, 1\}, E_2, T_2)$ shown in Fig. 1, with $E_2 = \{-1, 0, 1\}$ and $T_2 = \{0 \xrightarrow{0} 0, 0 \xrightarrow{1} 1, 1 \xrightarrow{-1} 0, 1 \xrightarrow{0} 1\}$. A region $X \equiv (\sigma, \eta)$ determines an *atomic* elementary net $N_X = (\{X\}, E, F_X)$ with flow relation F_X set according to the mapping η, namely,

$$X \in {}^\bullet e \quad \text{iff} \quad \eta(e) = -1 \quad \text{and} \quad X \in e^\bullet \quad \text{iff} \quad \eta(e) = 1.$$

[3] A morphism of transition systems $(\sigma, \eta) : (S_1, E_1, T_1) \to (S_2, E_2, T_2)$ is a pair of mappings $\sigma : S_1 \to S_2$ and $\eta : E_1 \to E_2$ such that $s \xrightarrow{e} s' \in T_1 \Rightarrow \sigma s \xrightarrow{\eta e} \sigma s' \in T_2$.



$$X \equiv (\sigma, \eta) : \mathbf{T} \to \mathbf{2}$$

Fig. 1. Regions as morphisms.

If $X = [\![x]\!]_P$ is the extension of a place x of a net $N = (P, E, F)$ then N_X is just the atomic subnet of N induced by x.

Given a transition system $\mathrm{T} = (S, E, T)$, an elementary net T^* may now be *synthesized* from the set $\mathbf{R}(\mathrm{T})$ of regions of T by amalgamating on E all the atomic nets N_X for X ranging over $\mathbf{R}(\mathrm{T})$. Thus, the net synthesized from T is $\mathrm{T}^* = \sum_{X \in \mathbf{R}(\mathrm{T})} N_X$. Every region X of T expresses an *elementary synchronic constraint* on event behaviours, satisfied in all possible runs of T. For instance, the region depicted in Fig. 1 expresses the constraint that two successive occurrences of event b should be separated by one occurrence of event a and vice versa. If we supply T with an initial state $s_0 \in S$, then the elementary net N (and each of its atomic components N_X) comes equipped with an initial marking $M_0 \subseteq 2^{\mathbf{R}(\mathrm{T})}$, containing exactly those regions which the initial state belongs to: $X \in M_0$ if and only if $s_0 \in X$. $\mathscr{A}^* = (\mathrm{T}^*, M_0)$ is the elementary net system *synthesized* from the automaton $\mathscr{A} = (\mathrm{T}, s_0)$. Suppose for instance that the initial state does not belong to the region represented in Fig. 1; then the unique place of the induced atomic net N_X is not marked initially, and the language of the atomic net system $\mathscr{N}_X$ is the shuffle of $(a \cdot b)^*$ and c^*. Since the regions of T are the morphisms $(\sigma, \eta) : \mathrm{T} \to 2$, the language of $\mathscr{A}$ is included in the language of every atomic net system $\mathscr{N}_X$ induced from $X \in \mathbf{R}(\mathrm{T})$ and thus it is included in their intersection i.e. in the language of $\mathscr{A}^*$. Adding up synchronic constraints imposed by regions amounts in fact to intersecting behaviours. The state graphs of elementary net systems are precisely those automata whose behaviour may be totally specified in terms of elementary synchronic constraints (see Theorem 10 below).

2.3. Elementary transition systems

This section reports on Ehrenfeucht and Rozenberg's characterization of isomorphism classes of state graphs of elementary net systems as *elementary* transition systems, i.e. transition systems owning *admissible* sets of regions as defined by Desel and Reisig.

Let $\mathscr{A} = (S, E, T, s_0)$ be isomorphic to the state graph of some elementary net system $\mathscr{N} = (P, E, F, M_0)$. If s_1 and s_2 are two distinct states of S, viewed as markings of $\mathscr{N}$, then there exists a place $x \in P$ which belongs to exactly one of these markings; hence there exists a region (the extension of the place x) that distinguishes between s_1 and s_2. If an event e has not concession at a given state s, viewed as a marking $M = [\![s]\!]_S$, then either ${}^\bullet e \not\subseteq M$ or $e^\bullet \cap M \neq \emptyset$; hence there exists a region $X \equiv (\sigma, \eta)$ such that $\sigma(s) = 0$ and $\eta(e) = -1$ (in the first case, X is the extension of a place $x \in {}^\bullet e \setminus M$, and in the second case it is the complement of the extension of a place $x' \in e^\bullet \cap M$). Let $R_s = \{X \in \mathbf{R}(\mathscr{A}) / s \in X\}$ denote the set of (non trivial) regions of $\mathscr{A}$ containing state s, and let now ${}^\bullet e$ denote the set of regions $X \equiv (\sigma, \eta)$ of $\mathscr{A}$ such that $\eta(e) = -1$, then:

Observation 8. *The following two* separation axioms *are satisfied in every state graph* $\mathscr{A}$:

1. $\forall s, s' \in S \; R_s = R_{s'} \Rightarrow s = s'$,
2. $\forall s \in S \; \forall e \in E \; {}^\bullet e \subset R_s \Rightarrow s \xrightarrow{e}$

Definition 9 (*Elementary transition system*). An elementary transition system is an automaton that fulfils the four conditions stated in Observation 6 plus the above two separation axioms.

Theorem 10 (Ehrenfencht and Rozenberg [8]). *An automaton is the state graph of an elementary net system if and only if it is an elementary transition system, and in that case* $\mathscr{A} \cong \mathscr{A}^{**}$.

Notice that the complement $\overline{X} = S \setminus X$ of a region X is a region with dual flow relations: $X \in {}^\bullet e \Leftrightarrow \overline{X} \in e^\bullet$ and $X \in e^\bullet \Leftrightarrow \overline{X} \in {}^\bullet e$. Even though the marking graph of an elementary net system $\mathscr{N}$ is always isomorphic to the marking graph of $\mathscr{N}^{**}$, $\mathscr{N}$ is generally embedded in $\mathscr{N}^{**}$ as a strict subnet with fewer conditions (the embedding maps a condition x to the region X of the marking graph formed of all markings containing that condition).

Definition 11. An elementary net system $\mathscr{N}$ is said to be *saturated* if $\mathscr{N} \equiv \mathscr{N}^{**}$, or equivalently, if $\mathscr{N} \equiv \mathscr{A}^*$ for some elementary transition system $\mathscr{A}$.

Example 12. Consider the elementary net system shown in Fig. 2. Its marking graph is shown in Fig. 3, where

$$s_0 = \{x_1; x; y_1\}$$

$$s_1 = \{x_2; y_1\}$$

$$s_2 = \{x_1; y_2\}$$

$$s_3 = \{x_3; x; y_1\}$$

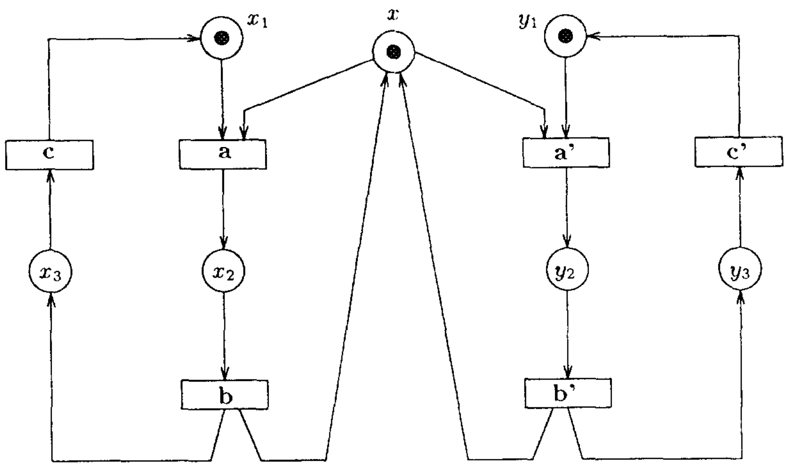


Fig. 2. An elementary net system for mutual exclusion.

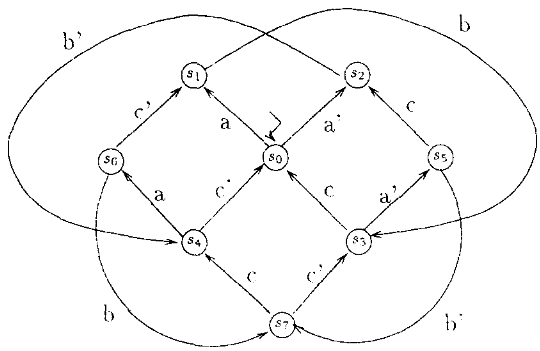


Fig. 3. The state graph of the elementary net system of Fig. 2.

$$s_4 = \{x_1; x; y_3\}$$

$$s_5 = \{x_3; y_2\}$$

$$s_6 = \{x_2; y_3\}$$

$$s_7 = \{x_3; x; y_3\}$$

Some (non-trivial) regions of that elementary transition system are shown in Fig. 4. The missing items can be obtained by symmetry. In each drawing, the grey states form a region, say X, the flow arcs attached to this region X and to the complementary region $\overline{X}$ are indicated, and one token is put in the place X or $\overline{X}$ that contains the initial state. Altogether, one ends up with the elementary net system shown in Fig. 5. This net $\mathcal{N}^{**}$ is the saturated version of the net $\mathcal{N}$ shown in Fig. 2 and their respective marking graphs are both isomorphic to the graph $\mathcal{N}^{*}$ shown in Fig. 3. Observe the embedding of $\mathcal{N}$ into $\mathcal{N}^{**}$ via the function $x \to [\![x]\!]$ that maps places to their extensions. The

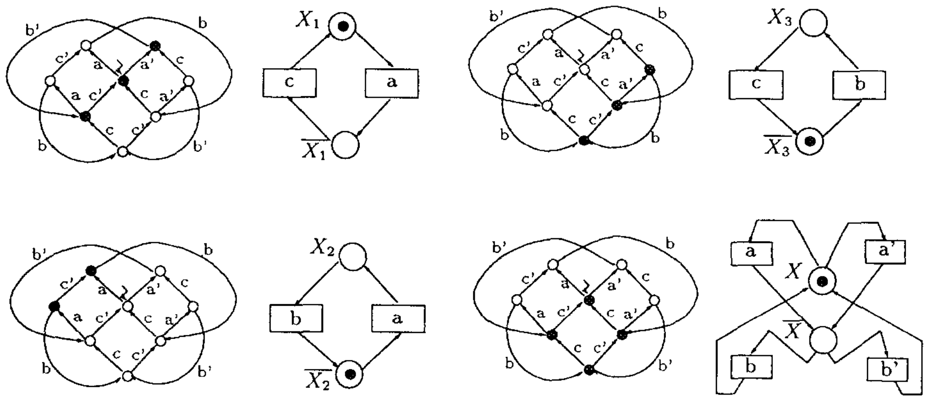


Fig. 4. Some regions of the elementary transition system of Fig. 3.

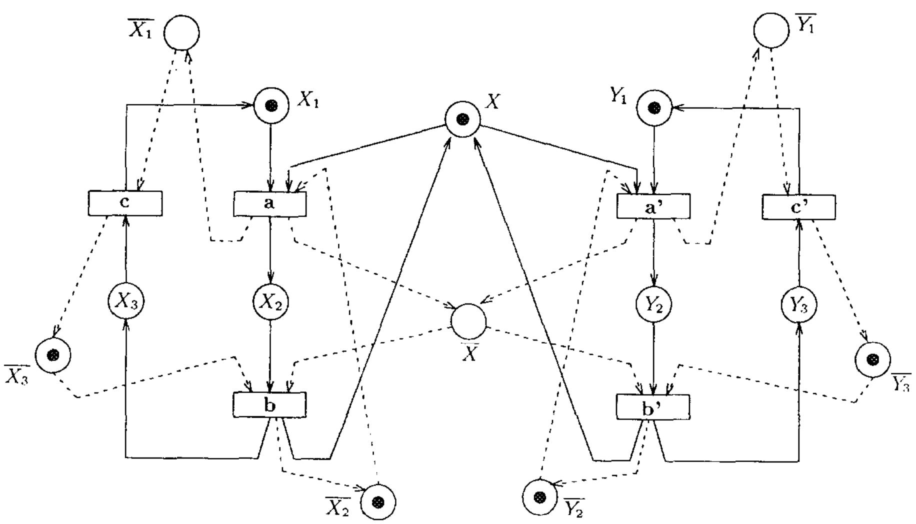


Fig. 5. The elementary net system synthesized from the elementary transition system of Fig. 3.

set of places of $\mathcal{N}^{**}$ (or regions of the marking graph $\mathcal{N}^{*}$) may be enumerated as follows:

$$
\begin{array}{lll}
X = \llbracket x \rrbracket = \{s_0; s_3; s_4; s_7\} & \quad & \overline{X} = \{s_1; s_2; s_5; s_6\} \\
X_1 = \llbracket x_1 \rrbracket = \{s_0; s_2; s_4\} & & \overline{X_1} = \{s_1; s_3; s_5; s_6; s_7\} \\
X_2 = \llbracket x_2 \rrbracket = \{s_1; s_6\} & & \overline{X_2} = \{s_0; s_2; s_3; s_4; s_5; s_7\} \\
X_3 = \llbracket x_3 \rrbracket = \{s_3; s_5; s_7\} & & \overline{X_3} = \{s_0; s_1; s_2; s_4; s_6\} \\
Y_1 = \llbracket y_1 \rrbracket = \{s_0; s_1; s_3\} & & \overline{Y_1} = \{s_2; s_4; s_5; s_6; s_7\} \\
Y_2 = \llbracket y_2 \rrbracket = \{s_2; s_5\} & & \overline{Y_2} = \{s_0; s_1; s_3; s_4; s_6; s_7\} \\
Y_3 = \llbracket y_3 \rrbracket = \{s_4; s_6; s_7\} & & \overline{Y_3} = \{s_0; s_1; s_2; s_3; s_5\}
\end{array}
$$

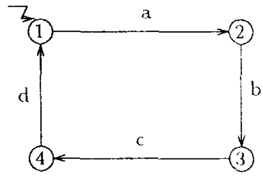


Fig. 6. The four seasons.

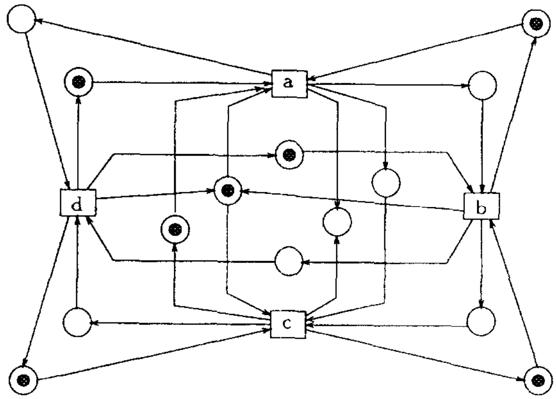


Fig. 7. The four seasons saturated net system.

Definition 13. Given an automaton $\mathscr{A}$, a subset of regions $R \subseteq \mathbf{R}(\mathscr{A})$ is said to be *admissible* if $\mathscr{A} \equiv \mathscr{N}^*$ for $\mathscr{N}$ defined as $\sum_{X \in R} \mathscr{N}_X$.

Proposition 14. *Any set of regions that contains an admissible set of regions is admissible.*

Therefore, as soon as an admissible set of regions has been computed in an elementary transition system, adding new regions as places in the resulting net would not modify the behaviour of that net. One aspect of the synthesis problem is to find admissible sets of regions as small as possible. Notice that there is in general no least admissible set of regions as illustrated by the "four seasons" example shown in Fig. 6. Actually, the saturated net system synthesized from that elementary transition system, depicted in Fig. 7, contains two minimal subnet systems, shown in Fig. 8, which still have the same behaviour (this example is borrowed from [6]). In order to construct an admissible set of regions in $\mathscr{A}$, it suffices to collect witnesses for the satisfaction of all the instances in $\mathscr{A}$ of the two axioms of separation which have been stated in Observation 8.

Proposition 15 (Desel and Reisig [6]). *Given $\mathscr{A} = (S, E, T, s_0)$, $s \in S$, and $R' \subseteq \mathbf{R}(\mathscr{A})$, let $R'_s = \{X \in R' / s \in X\}$ i.e. $R'_s = R_s \cap R'$, then R' is an admissible set of regions of*

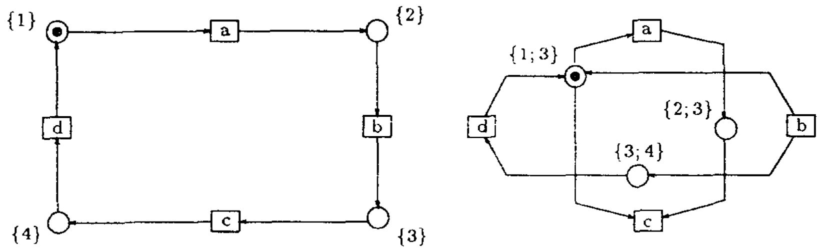


Fig. 8. Two elementary net systems assembled from minimal admissible sets of regions.

$\mathscr{A}$ if and only if the following are satisfied:

1. $\forall s, s' \in S\ R'_s = R'_{s'} \Rightarrow s = s'$,
2. $\forall s \in S\ \forall e \in E\ ({}^\bullet e \subset R'_s \wedge e^\bullet \cap R'_s = \emptyset) \Rightarrow s \xrightarrow{e}$

In order to decide whether a finite automaton $\mathscr{A} = (S, E, T, s_0)$ satisfying the conditions stated in Observation 6 is elementary, it is therefore enough to compute at most $|S| \times (|S| \times |E|)$ regions in $\mathscr{A}$.

Corollary 16. *If $\mathscr{A} = (S, E, T, s_0)$ is an elementary transition system, there must exist an elementary net system $\mathscr{N}$ with at most $|S| \times (|S| \times |E|)$ places such that $\mathscr{N}^* \equiv \mathscr{A}$.*

2.4. From the separation axioms to boolean equations

This section lays the ground for the complexity analysis to be discussed in Section 3, with the intent to focus the attention of the reader on the algebraic contents of the synthesis problem. We show that this decision problem may be encoded to systems of polynomial equations over the boolean ring. A similar algebraic setting is used in [13] for the polynomial time synthesis of the so-called flip–flop nets, with the main difference that all the equations used there are linear.

In view of the above, solving the synthesis problem for elementary net systems amounts to solving a quadratic (in the size of the automaton) number of instances of the following two separation problems.

States Separation Problem (SSP):
Given $\mathrm{T} = (S, E, T)$ and a pair of distinct states $(s_1, s_2) \in S \times S$, find a region X such that $s_1 \in X$ if and only if $s_2 \notin X$.

Event/State Separation Problem (ESSP):
Given $\mathrm{T} = (S, E, T)$ and a pair $(s, e) \in S \times E$ such that e *has no concession* at s ($s \xrightarrow{e} s'$ in T for no $s' \in S$), find a region X *inhibiting* e at s in the sense that $X \in {}^\bullet e$ and $s \notin X$.

Now, problems SSP and ESSP are in NP, as one may certainly check in polynomial time whether a given region solves a fixed instance of the separation problems, and the synthesis problem for elementary net systems is therefore in NP. Hiraishi proved in fact that both problems SSP and ESSP are NP-complete [11], but as he remarked, it does not follow therefrom that the synthesis problem for elementary net systems is NP-complete. The purpose of Section 3 is to establish this result.

Let us now proceed to the encoding of the separation problems into equations over the boolean ring $\mathbb{Z}/2\mathbb{Z}$.

Definition 17. The second projections $\eta : E \to \{-1,0,1\}$ of regions (σ,η) are called *signed regions*, and the maps $\rho : E \to \{0,1\}$ defined from signed regions by $\rho(e) = |\eta(e)|$ are called *abstract regions*.

Given a region (σ,η), the abstract region $\rho = |\eta|$ indicates which transition labels entail a change of the current value for σ:

$$s \xrightarrow{e} s' \in T \Rightarrow [\sigma(s) \neq \sigma(s') \Leftrightarrow \rho(e) = 1] \tag{1}$$

The abstract regions of a transition system (S,E,T) are elements of the $\mathbb{Z}/2\mathbb{Z}$-module $(E \to \mathbb{Z}/2\mathbb{Z})$ which consists of the set of mappings from E to $\mathbb{Z}/2\mathbb{Z}$, but beware of the fact that they do not always form a submodule of that module! For instance, $\rho'(a) = 1$, $\rho'(b) = 0$ and $\rho''(a) = 0$, $\rho''(b) = 1$ both define abstract regions in the transition system $(\{s_0,s_1,s_2,s_3\}, \{a,b\}, T)$ with $T = \{s_0 \xrightarrow{a} s_1, s_1 \xrightarrow{b} s_2, s_0 \xrightarrow{b} s_3, s_3 \xrightarrow{a} s_2\}$, whereas their sum $\rho' + \rho''$ is not an abstract region.

Observation 18. *In a connected transition system, an abstract region determines always two complementary regions.*

In view of this remark, the main step towards a translation of the separation axioms to equations is to produce an algebraic characterization for the abstract regions of a given transition system $\mathrm{T} = (S,E,T)$. For that purpose, we shall use classical techniques from graph theory, adapted to labelled graphs $[S,T]$ with labelling function $\ell : T \to E : \ell(s \xrightarrow{e} s') = e$. Let us recall some basic graph terminology.

Definition 19 (*Graphs*). A *graph* $G = [S,T]$ is given by a set S of *nodes*, a set T of *transitions* (or arcs), together with two maps $\partial^0, \partial^1 : T \to S$, indicating respectively the *source* and *target* of transitions. A *path* in G is a finite sequence of transitions $t_1 \ldots t_k$ where $\partial^1(t_i) = \partial^0(t_{i+1})$ for $i < k$. Nodes $\partial^0(t_1)$ and $\partial^1(t_k)$ are the *extremities*, or respectively the *initial* and *terminal* nodes of the path. A *chain* in G is a path in the graph $[S, T + T^{-1}]$, where $\partial^0(t^{-1}) = \partial^1(t)$ and $\partial^1(t^{-1}) = \partial^0(t)$ for $t \in T$. A *cycle* is a chain with identical extremities. A cycle which is a path is *directed*. A *rooted* graph is a graph with a distinguished node, called the *initial* node. Paths from the initial node are *initial* paths.

An essential property of abstract regions is to map cycles to 0 in $\mathbb{Z}/2\mathbb{Z}$. We need introducing further notations before we can state that property. As usual, a chain c will be represented as a vector $c \in (T \to \mathbb{Z})$, where $c(t)$ is the algebraic number of occurrences

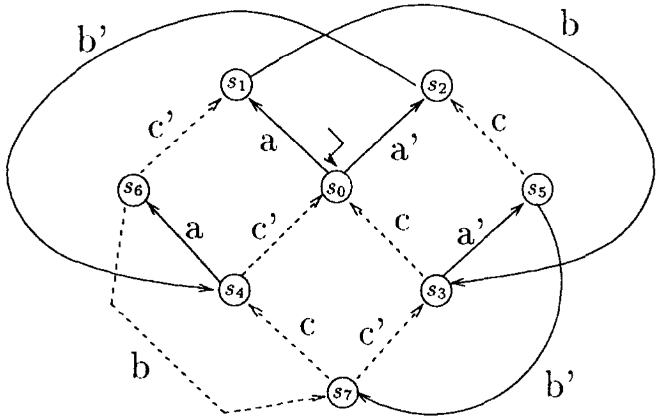


Fig. 9. A graph and one of its maximal trees.

of transition t in c (i.e. $\varepsilon(t) = 0$, $(t \cdot c)(t) = 1 + c(t)$ and $(t^{-1} \cdot c)(t) = c(t) - 1$). Vectors in this $\mathbb{Z}$-module will be represented as formal sums: $c = \sum c_j \cdot t_j$ where $c_j = c(t_j)$. The *Parikh image* of a chain $c = \sum c_j \cdot t_j$ is the vector $\pi(c) = \sum c_j \cdot \ell(t_j)$ evaluated as an element of the $\mathbb{Z}$-module $(E \to \mathbb{Z})$, hence $\pi(c)(e) = \sum\{c_j \mid \ell(t_j) = e\}$. We recall that the *scalar product* of two vectors $\alpha = \sum \alpha_i \cdot x_i$ and $\beta = \sum \beta_i \cdot x_i$ of a $\mathbb{Z}$-module $(X \to \mathbb{Z})$ is the integer $\alpha \cdot \beta = \sum \alpha_i \cdot \beta_i$. The *Parikh image modulo* 2 of a chain $c = \sum c_j \cdot t_j$ is the vector $\pi_2(c) = \sum c_j \cdot \ell(t_j)$ evaluated as an element of the $\mathbb{Z}/2\mathbb{Z}$ module $E \to \mathbb{Z}/2\mathbb{Z}$.

So for notations. Let us recall a classical fact about cycles in a graph: they form a submodule of the module of chains in that graph. In the case of a connected graph $[S, T]$, the classical construction of a basis for that submodule is as follows: let $U \subseteq T$ be a maximal tree, then each transition $t \in T \setminus U$ determines a unique cycle $c^t \in (U \cup \{t\}) \to \mathbb{Z}$, and $\{c^t \mid t \in T \setminus U\}$ is a basis for the $\mathbb{Z}$-module of cycles in $[S, T]$.

Example 20. Fig. 9 displays a graph and a maximal tree in that graph. There are 7 transitions which are not part of the maximal tree: $t_1 = s_5 \xrightarrow{c} s_2$, $t_2 = s_3 \xrightarrow{c} s_0$, $t_3 = s_7 \xrightarrow{c} s_4$ $t_4 = s_6 \xrightarrow{c'} s_1$, $t_5 = s_4 \xrightarrow{c'} s_0$ $t_6 = s_7 \xrightarrow{c'} s_3$, and $t_7 = s_6 \xrightarrow{b} s_7$. For instance, the transition $t_1 = s_5 \xrightarrow{c} s_2$ determines the cycle

$$c^{t_1} = (s_0 \xrightarrow{a} s_1) + (s_1 \xrightarrow{b} s_3) + (s_3 \xrightarrow{a'} s_5) + (s_5 \xrightarrow{c} s_2) - (s_0 \xrightarrow{a'} s_2)$$

with Parikh image $\pi(c^{t_1}) = a + b + c$. One can verify that $\pi(c^{t_1}) = \pi(c^{t_2}) = \pi(c^{t_3})$ $= a + b + c$, $\pi(c^{t_4}) = \pi(c^{t_5}) = \pi(c^{t_6}) = a' + b' + c'$, and $\pi(c^{t_7}) = 0$.

Let us now state the essential property of abstract regions:

Proposition 21. *If* $\rho : E \to \mathbb{Z}/2\mathbb{Z}$ *is an abstract region of the transition system* (S, E, T) *then* $\rho \cdot \pi_2(c) = 0$ *in* $\mathbb{Z}/2\mathbb{Z}$ *for every cycle* c *in the graph* $[S, T]$.

Proof. Let ρ be an abstract region of (S,E,T). By the definition of abstract regions, there exists a region (σ,η) such that $\rho(e)=|\eta(e)|$ for every $e\in E$. By the definition of regions, $s\xrightarrow{e}s'\in T\Rightarrow\sigma(s')=\sigma(s)+\rho(e)$ in $\mathbb{Z}/2\mathbb{Z}$, or yet equivalently $\sigma(s)+\sigma(s')=\rho(e)$. By induction on the length of chains, $\sigma(s)+\sigma(s')=\rho\cdot\pi_2(c)$ for every chain with extremities s and s' (where $\pi_2(c)$ is a Parikh image modulo 2), and the expected result follows as a particular case since $s=s'\Rightarrow\sigma(s)+\sigma(s')=0$ in $\mathbb{Z}/2\mathbb{Z}$. □

This fundamental property taken alone does not provide a full characterization for abstract regions. This is quite clear since we already know that abstract regions in a transition system (S,E,T) do not always form a submodule of the $\mathbb{Z}/2\mathbb{Z}$-module $E\to\mathbb{Z}/2\mathbb{Z}$: non-linear equations are needed! In the sequel, we consider a fixed automaton $\mathscr{A}=(S,E,T,s_0)$ and a maximal tree $U\subseteq T$ rooted at s_0. For each $s\in S$, we let c_s be the branch from s_0 to s in that tree, and we let $\pi_s=\pi_2(c_s)$ denote its Parikh image modulo 2. Now suppose that $|\eta(e)|=1$ for some region (σ,η) such that e has concession at states s and s', then necessarily $\sigma(s)=\sigma(s')$ by definition of regions. In $\mathbb{Z}/2\mathbb{Z}$, this may be expressed by the non-linear equation

$$\rho(e)\times[\rho\cdot(\pi_s+\pi_{s'})]=0$$

where $\rho(e')=|\eta(e')|$ for all $e'\in E$. We obtain in this way a full characterization for abstract regions:

Proposition 22. *A map $\rho:E\to\mathbb{Z}/2\mathbb{Z}$ is an abstract region if and only if it satisfies*

$$\rho\cdot\pi_2(c^t)=0 \tag{2}$$

$$\rho(e)\times[\rho\cdot(\pi_s+\pi_{s'})]=0 \tag{3}$$

for every cycle c^t in the basis of cycles, for every event $e\in E$, and for every pair of states s and s' in S at which e has concession.

Proof. The condition is clearly necessary. Conversely, if Eq. (2) holds, one can define a map $\sigma:S\to\{0,1\}$ by $\sigma(s)=\rho\cdot\pi_s$. Now assume $\rho(e)=1$ for some event e enabled at states s and s'. If Eq. (3) holds, $\sigma(s)$ and $\sigma(s')$ are identical, hence we can define σ_e as the common value of $\sigma(s)$ for all states s enabling e. A region (σ,η) such that $\rho=|\eta|$ is obtained by setting $\eta(e)=0$ if $\rho(e)=0$, $\eta(e)=1$ if $\rho(e)=1$ and $\sigma_e=0$, and $\eta(e)=-1$ if $\rho(e)=1$ and $\sigma_e=1$. □

Example 23 (*continued*). In our running example, the Parikh images of the cycles are $a+b+c$, $a'+b'+c'$ and 0, hence the equations of type (2) are

$$\rho(a)+\rho(b)+\rho(c)=0 \quad\text{and}\quad \rho(a')+\rho(b')+\rho(c')=0 \tag{4}$$

which determine altogether a four dimensional $\mathbb{Z}/2\mathbb{Z}$-module with basis as follows:

$$\rho_1=a+c;\quad \rho_2=b+c;\quad \rho_3=a'+c';\quad \rho_4=b'+c'$$

Table 1
Regions X_ρ defined from abstract regions ρ

$\rho \cdot \pi_s$	s_0	s_1	s_2	s_3	s_4	s_5	s_6	s_7
ρ_1	0	1	0	1	0	1	1	1
ρ_2	0	0	0	1	0	1	0	1
ρ_3	0	0	1	0	1	1	1	1
ρ_4	0	0	0	0	1	0	1	1
$\rho_1 + \rho_2$	0	1	0	0	0	0	1	0
$\rho_3 + \rho_4$	0	0	1	0	0	1	0	0
$\rho_1 + \rho_2 + \rho_3 + \rho_4$	0	1	1	0	0	1	1	0

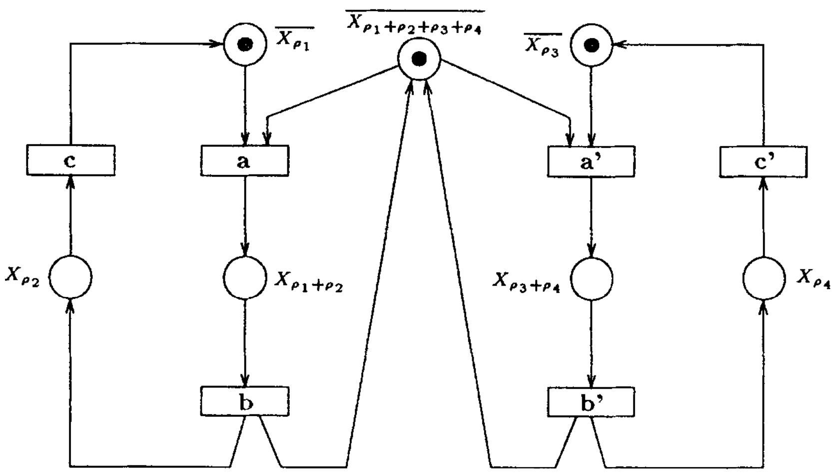


Fig. 10. The net synthesized from the (admissible) set of abstract regions.

A linear combination ρ of these vectors is an abstract region of the graph shown in Fig. 9 if and only if it satisfies the non-linear equations of type (3) which modulo the Eqs. (4) read:

$$\rho(a) \times \rho(c') = \rho(b) \times \rho(c') = \rho(c) \times \rho(c') = \rho(c) \times \rho(a') = \rho(c) \times \rho(b') = 0$$

Seven out of the 2^4 elements of the $\mathbb{Z}/2\mathbb{Z}$-module spanned by $(\rho_1, \rho_2, \rho_3, \rho_4)$ are abstract regions (they are indicated as the row entries of Table 1). Each abstract region ρ determines two complementary regions X_ρ and $\overline{X_\rho}$, where $X_\rho = \{s \in S \mid \rho \cdot \pi_s = 1\}$ and therefore $s_0 \notin X_\rho$. The states s_0 to s_7 are represented by vectors π_s as follows:

$$\begin{array}{llll} \pi_{s_0} = 0 & \pi_{s_1} = a & \pi_{s_2} = a' & \pi_{s_3} = a + b \\ \pi_{s_4} = a' + b' & \pi_{s_5} = a + b + a' & \pi_{s_6} = a' + b' + a & \pi_{s_7} = a + b + a' + b' \end{array}$$

The resulting regions X_ρ, tabulated in Table 1, are half of the 14 regions of Fig. 5; the correspondence is made explicit in Fig. 10.

Let us finally indicate the equational encoding for the instances of the separation problems SSP and ESSP.

Definition 24. An abstract region ρ separates the states s and s' if it satisfies the equation

$$\rho \cdot (\pi_s + \pi_{s'}) = 1 \tag{5}$$

An abstract region ρ inhibits event e at state s if it satisfies the equations

$$\rho(e) = 1 \tag{6}$$

$$\rho \cdot (\pi_s + \pi_{s'}) = 1 \tag{7}$$

where s' is some arbitrary state enabling e. A set R of abstract regions is *admissible* if it provides a separating region for every pair of distinct states (s, s') and an inhibiting region for every pair (s, e) such that event e has no concession at state s.

An admissible set of regions may always be constructed from an admissible set of abstract regions: if ρ separates states s and s' then both X_ρ and $\overline{X_\rho}$ separate s and s'; if ρ inhibits event e at state s then either X_ρ or $\overline{X_\rho}$ inhibits e at s (in our running example, the full set of abstract regions is admissible, but no strict subset of that set is admissible).

Proposition 25. *An automaton is the state graph of an elementary net system if and only if it may be fitted with an admissible set of abstract regions.*

3. The synthesis problem is NP-hard

We have seen in Section 2 that the synthesis problem for elementary net systems is in NP. We will show at present that it is NP-hard, thus establishing the following.

Theorem 26. *The synthesis problem for elementary net systems is* NP*-complete.*

In order to achieve this goal, we construct a polynomial reduction of 3-SAT to the synthesis problem. Recall that 3-SAT is the problem whether, given a finite set V of boolean variables and a finite system C of (disjunctive) clauses over V, with exactly three literals per clause, there exists a truth assignment for V satisfying all clauses in C. Problem 3-SAT is known to be NP-complete, see e.g. [9]. We shall reduce 3-SAT to the synthesis problem for elementary net systems by encoding uniformly systems of clauses (V, C) to automata $\mathscr{A}(V, C)$, with size polynomial in the size of (V, C), such that (V, C) is satisfiable if and only if $\mathscr{A}(V, C)$ is an elementary transition system. This reduction is done in two stages. First, we reduce 3-SAT to satisfiability of systems of additive or multiplicative clauses over the boolean ring, a structure well suited for expressing the separation problems as we saw in Section 2. Second, we encode systems of clauses over the boolean ring to transition systems, and we classify regions in the latter with respect to solutions of the former. We finally prove that satisfiability of systems of clauses over the boolean ring reduces through this polynomial encoding to the solvability of all instances of the separation problems for transition systems, and hence to the synthesis problem for elementary net systems.

3.1. Systems of clauses over the boolean ring

The following definition is introduced for the specific purpose of this paper.

Definition 27 (*Systems of clauses over the boolean ring*). Let $X = \{x_0, \dots, x_n\}$ be a finite set of boolean variables, with a distinguished element x_0. A *system of clauses over the boolean ring* is a pair (Σ, Π) where Σ is a finite set of additive clauses σ_α $(\alpha \in A)$ and Π is a finite set of multiplicative clauses π_β $(\beta \in B)$ with respective forms $x_{\alpha_0} + x_{\alpha_1} + x_{\alpha_2}$ and $x_{\beta_1} \cdot x_{\beta_2}$, subject to the following restrictions: each additive clause has exactly three variables, two additive clauses have at most one common variable, each multiplicative clause has exactly two variables, and the distinguished variable x_0 does not occur in any multiplicative clause. The system (Σ, Π) is said to be *satisfiable* if there exists a truth assignment for X such that $x_0 = 1$, $\sigma_\alpha = 0$ for all $\alpha \in A$, and $\pi_\beta = 0$ for all $\beta \in B$. Such a truth assignment is called a solution of (Σ, Π).

Observe that in the boolean ring, the equations $z_0 = z_1 + \cdots + z_n$ and $z_0 + z_1 + \cdots + z_n = 0$ are equivalent in view of the inversion law $z + z = 0$. Using this remark, each instance of problems SSP and ESSP may be reduced to the satisfiability of a corresponding system of clauses, with size polynomial in the size of the transition system.

Let CBR denote the satisfiability problem for systems of clauses over the boolean ring. CBR reduces polynomially to 3-SAT by expanding each additive clause $a + b + c$ to a set of 4 clauses $\{a \vee b \vee c,\ \neg a \vee \neg b \vee c,\ \neg a \vee b \vee \neg c,\ a \vee \neg b \vee \neg c\}$ and each multiplicative clause ab to a set of 2 clauses $\{a \vee a \vee a,\ b \vee b \vee b\}$. Conversely:

Proposition 28. *3-SAT reduces polynomially to CBR.*

Proof. Let (V, C) be an instance of 3-SAT. Define $W = V \cup \neg V$ where $\neg V = \{\neg v \mid v \in V\}$, and equip this set with the involution $\neg(v) = \neg v$ and $\neg(\neg v) = v$ for $v \in V$. We construct from (V, C) a system of clauses (Σ, Π) over the boolean ring, with variables in the set $X = \{x_0\} \cup W \cup (W \times W)$, such that every truth assignment for V which satisfies C extends to a truth assignment for X which satisfies (Σ, Π) by setting $[\![\neg v]\!] = \neg[\![v]\!]$ for $v \in V$ and $[\![ab]\!] = [\![a]\!] \wedge [\![b]\!]$ for $a, b \in W$, and every truth assignment for X which satisfies (Σ, Π) restricts to a truth assignment for V which satisfies C. The additive clauses in Σ are defined as follows: for each literal $c \in W$ set the clause $x_0 + c + \neg c$, and for each pair of literals $ab \in W \times W$ set the clause $a + ab + a\neg b$. The multiplicative clauses in Π are defined as follows: for each pair of literals $ab \in W \times W$ set the two clauses $\neg a \cdot ab$ and $\neg b \cdot ab$, and for each disjunctive clause $a \vee b \vee c$ in C set the clause $\neg a \cdot \neg b \neg c$. □

3.2. Encoding systems of clauses over the boolean ring to labelled transition systems

The purpose of the section is to encode uniformly systems of clauses (Σ, Π) over the boolean ring to automata $\mathscr{A}(\Sigma, \Pi)$ with size polynomial in the size of (Σ, Π), such that (Σ, Π) is satisfiable if and only if $\mathscr{A}(\Sigma, \Pi)$ is an elementary transition system. The encoding is done in two stages. In the first stage, we construct from (Σ, Π) a system of equations (Σ', Π') with a larger set of variables, and we state the relationships between the respective solutions of (Σ, Π) and (Σ', Π'). In the second stage, we construct from (Σ', Π') an automaton $\mathscr{A}(\Sigma, \Pi)$ and we observe that (Σ, Π) is satisfiable if $\mathscr{A}(\Sigma, \Pi)$ is elementary. The proof for the converse is left to a later section.

Let $X = \{x_0, \dots, x_{n-1}\}$ be the set of variables of (Σ, Π), where the respective sets of clauses $\Sigma = \{\sigma_\alpha \mid \alpha \in A\}$ and $\Pi = \{\pi_\beta \mid \beta \in B\}$ have typical elements

$$(\sigma_\alpha): \quad x_{\alpha_0} + x_{\alpha_1} + x_{\alpha_2}; \qquad (\pi_\beta): \quad x_{\beta_1} \cdot x_{\beta_2}.$$

Let $X' = X \cup \{x^\alpha \mid \alpha \in A\} \cup \{x_n, \dots, x_N\}$, where $N - n + 1 = 3 \times \mathit{size}(A)$. Define $\Sigma' = \{\sigma'_\alpha \mid \alpha \in A\} \cup \{\sigma''_\alpha \mid \alpha \in A\}$, where σ'_α and σ''_α are the equations:

$$(\sigma'_\alpha): \quad x_{\alpha_0} + x_{\alpha_1} + x_{\alpha_2} + x_{\alpha_3} + x_{\alpha_4} + x_{\alpha_5} = 0,$$

$$(\sigma''_\alpha): \quad x^\alpha + x_{\alpha_3} + x_{\alpha_4} + x_{\alpha_5} = 0$$

where $\{x_n, \dots, x_N\} = \bigcup_{\alpha \in A} \{x_{\alpha_3}, x_{\alpha_4}, x_{\alpha_5}\}$. Define $\Pi' = \{\pi_\alpha \mid \alpha \in A\} \cup \{\pi_\beta \mid \beta \in B\}$, where π_α and π_β are the equations:

$$(\pi_\alpha): \quad x_0 \cdot x^\alpha = 0; \qquad (\pi_\beta): \quad x_{\beta_1} \cdot x_{\beta_2} = 0.$$

A solution for (Σ', Π') is a truth assignment for X' such that all the above equations hold. A *distinguished solution* for (Σ', Π') is a solution which assigns value 1 to the distinguished variable x_0, and value 0 to all the auxiliary variables in $X' \setminus X$. Thus, every solution of (Σ, Π) extends to a distinguished solution of (Σ', Π'), and every distinguished solution of (Σ', Π') restricts to a solution of (Σ, Π). Before we construct $\mathscr{A}(\Sigma, \Pi)$, let us state some properties of the set of solutions of (Σ', Π') showing the degrees of freedom introduced by the auxiliary variables.

Fact 29. *For each positive integer $i \leqslant N$, there exists a family F_i of solutions $f : X' \to 2$ for (Σ', Π') such that for all $f \in F_i$ $f(x_i) = 1$ and for all $j \in \{0, \dots, N\}$ different from i there exists some $f \in F_i$ such that $f(x_j) = 0$.*

Proof. Given $i, j \in \{0, \dots, N\}$ such that $i \neq 0$ and $j \neq i$, we construct a solution $f : X' \to 2$ for (Σ', Π') such that $f(x_i) = 1$ and $f(x_j) = 0$. Suppose first that $1 \leqslant i \leqslant n-1$ and let $f : X \to 2$ be the valuation defined by $f(x_i) = 1$ and $f(x_k) = 0$ for $k \neq i$

(thus in particular $f(x_0)=0$). Let $f(\Sigma',\Pi')$ denote the system of equations over the residual variables in $X'\backslash X$ that proceeds from (Σ',Π') by replacing each occurrence of a variable $x \in X$ by the constant $f(x) \in 2$, then $f(\Sigma',\Pi')$ consists of the equations $x^\alpha = c^\alpha$ and $x_{\alpha_3}+x_{\alpha_4}+x_{\alpha_5} = c^\alpha$ for $\alpha \in A$, where c^α is the constant $c^\alpha = f(x_{\alpha_0})+f(x_{\alpha_1})+f(x_{\alpha_2})$ (all the equations in Π' degenerate to the trivial equation $0=0$). Hence f extends into a solution for (Σ',Π') where necessarily $f(x^\alpha)=c^\alpha$, but two variables in each set $\{x_{\alpha_3},x_{\alpha_4},x_{\alpha_5}\}$ can be chosen and assigned arbitrarily. Suppose now that $i \geqslant n$ and let $f : X \to 2$ be the valuation defined by $f(x_j)=0$ for all $j \in \{0,\dots,n-1\}$. Then $f(\Sigma',\Pi')$ consists of the equations $x^\alpha = x_{\alpha_3}+x_{\alpha_4}+x_{\alpha_5}=0$. Thus if j is different from i and belongs to $\{n,\dots,N\}$, f extends certainly into a solution for (Σ',Π') such that $f(x_j)$ =0. □

Fact 30. *For each $\alpha \in A$, there exists a family F_α of solutions $f : X' \to 2$ for (Σ',Π') such that for all $f \in F_\alpha$ $f(x^\alpha)=1$ and for all $j \in \{0,\dots,N\}$ there exists some $f \in F_\alpha$ such that $f(x_j)=0$.*

Proof. Let $\alpha \in A$ and $j \in \{0,\dots,N\}$. Choose $k_1 \in \{\alpha_0,\alpha_1,\alpha_2\}$ and $k_2 \in \{\alpha_3,\alpha_4,\alpha_5\}$ both different from j and 0. Let $f : X' \to 2$ be defined for $x \in X$ by $f(x_{k_1}) = f(x_{k_2}) = 1$ and $f(x_k)=0$ if $k \in \{0,\dots,N\} \setminus \{k_1,k_2\}$, and be defined for $x \in X'\backslash X$ by $f(x^\alpha)=1$ and $f(x^{\alpha'})=0$ if $\alpha' \in A \setminus \{\alpha\}$. This valuation is a solution for (Σ',Π'). Indeed (π_α) is satisfied because $f(x_0)=0$ and (π_β) is satisfied because $\beta_1,\beta_2 \in \{1,\dots,n-1\}$: at most one of the variables x_{β_1},x_{β_2} (the one such that $\beta_i = k_1$) is not assigned value 0. And of course, $f(x^\alpha)=1$ and $f(x_j)=0$. □

We now proceed to the definition of the automaton $\mathscr{A}(\Sigma,\Pi)$. This automaton will be assembled from a bunch of smaller automata, each of which encodes one equation in (Σ',Π'), tied together by a bunch of arcs $s_0 \xrightarrow{s_0^i} s_0^i$ originated from a fresh state s_0 and leading to their respective initial states s_0^i which are also used as fresh labels. Let us define precisely this operation of lifted union.

Definition 31. An automaton with *multiple initial states* is a transition system (S,E,T) with a set $S_0 \subseteq S$ of initial states. Given an i-indexed family of automata (S^i,E^i,T^i,S_0^i) such that $S^i \cap E^i = \emptyset$, their *union* $\cup_i(S^i,E^i,T^i,S_0^i)$ is the automaton $(\cup_i S^i, \cup_i E^i, \cup_i T^i, \cup_i S_0^i)$. Given an automaton (S,E,T,S_0) such that $S \cap E = \emptyset$, its *lift* is the automaton $(S',E',T',\{s_0\})$ with initial state s_0 ($\notin S$), set of states $S' = S \cup \{s_0\}$, set of events $E' = E \cup S_0$, and set of transitions $T' = T \cup \{s_0 \xrightarrow{s} s \mid s \in S_0\}$.

In order to enumerate the various components of the lifted union $\mathscr{A}(\Sigma,\Pi)$, we shall introduce five families indexed by $\alpha \in A$, $\beta \in B$ and $\gamma \in A \cup B$. The following notations will help us to trace back each variable $x_k \in X'$ to the equations σ'_α or π_β in which it occurs in Σ'. Recall that σ'_α and π_β are the respective equations $x_{\alpha_0}+\cdots+x_{\alpha_5}=0$ and $x_{\beta_1}\cdot x_{\beta_2}=0$, where the α_i and the β_j are fixed integers in $\{0,\dots,N\}$.

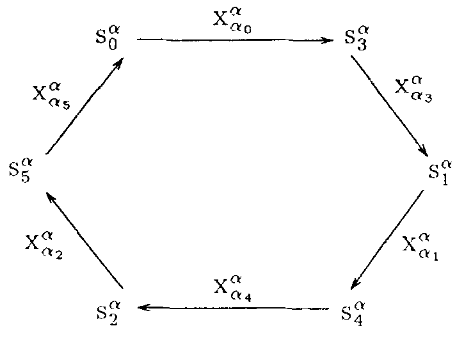


Fig. 11. S^α.

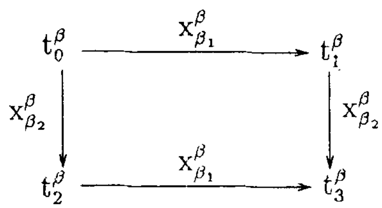


Fig. 12. T^β

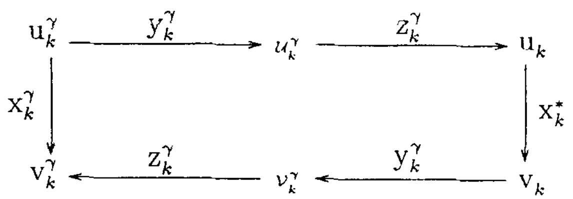


Fig. 13. UV_k^γ.

Notation 32. For k ranging over $\{0,\dots,N\}$, let $A(k)=\{\alpha\in A \mid \exists i\in\{0,\dots,5\} : k=\alpha_i\}$, $B(k)=\{\beta\in B \mid \exists j\in\{1,2\} : k=\beta_j\}$, and $\Gamma(k)=A(k)\cup B(k)$.

Definition 33. Let $\mathscr{A}(\Sigma,\Pi)$ and $\mathscr{A}'(\Sigma,\Pi)$ be, respectively, the lifted union and the union of the families of automata S^α, T^β, $UV_k = \cup_{\gamma\in\Gamma(k)} UV_k^\gamma$, $W^\alpha = W_L^\alpha \cup W_R^\alpha$ indexed by $\alpha\in A$, $\beta\in B$, and $k\in\{0,\dots,N\}$, where S^α, T^β, UV_k^γ, W_L^α, and W_R^α are the transition systems displayed in Figs. 11–14, with respective initial states s_0^α, t_0^β, u_k^γ, w_0^α, and w_3^α. $T(\Sigma,\Pi)$ and $T'(\Sigma,\Pi)$ denote the underlying transition systems of, respectively, $\mathscr{A}(\Sigma,\Pi)$ and $\mathscr{A}'(\Sigma,\Pi)$.

By inspection of Fig. 13 one observes the following.

Fact 34. *Let ρ be an abstract region of $T(\Sigma,\Pi)$ and $k\in[0,N]$, then $\forall\gamma\in\Gamma(k)$ $\rho(x_k^\gamma)=\rho(x_k^*)$, and the mapping $f: X'\to\mathbf{2}$ given by $f(x_k)=\rho(x_k^*)$ for $k\in[0,N]$, and $f(x^\alpha)=\rho(x_*^\alpha)$ for $\alpha\in A$ is a solution of the system of equations (Σ',Π').*

$$
\begin{tikzcd}
\mathrm{w}_0^\alpha \arrow[r, "\mathrm{x}_*^\alpha"] \arrow[d, "\mathrm{x}_0^*"'] \arrow[dr, phantom, "(W_L^\alpha)"] & \mathrm{w}_1^\alpha \arrow[d, "\mathrm{x}_0^*"] & \mathrm{w}_3^\alpha \arrow[r, "\mathrm{x}_{\alpha_3}^*"] \arrow[dr, phantom, "(W_R^\alpha)"] & \mathrm{w}_4^\alpha \arrow[d, "\mathrm{x}_{\alpha_4}^*"] \\
\mathrm{w}_2^\alpha \arrow[r, "\mathrm{x}_*^\alpha"'] & \mathrm{w}_7^\alpha & \mathrm{w}_6^\alpha \arrow[u, "\mathrm{x}_*^\alpha"] & \mathrm{w}_5^\alpha \arrow[l, "\mathrm{x}_{\alpha_5}^*"]
\end{tikzcd}
$$

Fig. 14. W^α.

Corollary 35. *(Σ, Π) is satisfiable if $\mathscr{A}(\Sigma, \Pi)$ is an elementary transition system.*

Proof. If $\mathscr{A}(\Sigma, \Pi)$ is an elementary transition system, there exists at least one region $R \equiv (\sigma_R, \eta_R)$ such that $\sigma_R(\mathrm{w}_0^\alpha) \neq \sigma_R(\mathrm{w}_2^\alpha)$ and thus $|\eta_R|(\mathrm{x}_0^*) = 1$. Then the abstract region $\rho = |\eta_R|$ induces a solution f of (Σ', Π') such that $f(x_0) = 1$ and which therefore restricts to a solution of (Σ, Π). $\square$

Observe that $\mathscr{A}(\Sigma, \Pi)$ is a transition system with size polynomial in the size of (Σ, Π) which satisfies the conditions of Observation 6. It is an elementary transition system if and only if all instances of the separation problems SSP and ESSP can be solved in $\mathrm{T}(\Sigma, \Pi)$. In order to prove that CBR reduces polynomially to the synthesis problem, it remains to show that $\mathscr{A}(\Sigma, \Pi)$ is elementary if (Σ, Π) is satisfiable. Thus, one should prove that every instance of SSP or ESSP can be solved in $\mathrm{T}(\Sigma, \Pi)$ or equivalently in $\mathrm{T}'(\Sigma, \Pi)$ if (Σ, Π) has a solution or yet equivalently if (Σ', Π') has a distinguished solution.

3.3. Satisfiability of systems of clauses reduces to the synthesis problem

We show in this section that every instance of SSP or ESSP can be solved in $\mathrm{T}'(\Sigma, \Pi)$ provided there exists a distinguished solution for (Σ', Π'). CBR reduces therefore to the synthesis problem for elementary net systems, and this problem is NP-complete as announced.

As a starting point, let us observe again that every region $R \equiv (\sigma_R, \eta_R)$ in $\mathrm{T}'(\Sigma, \Pi)$ determines a solution $f : X' \to \mathbf{2}$ for (Σ', Π'), given by $f(x_k) = |\eta_R|(\mathrm{x}_k^*)(= |\eta_R|(\mathrm{x}_k^\gamma))$ and $f(x^\alpha) = |\eta_R|(\mathrm{x}_*^\alpha)$. In order to carry on, we need a precise statement for the converse relationship, enabling us to construct sets of regions from arbitrary (i.e. possibly not distinguished) solutions of (Σ', Π').

Notation 36. In order to simplify the notation, let $T' = \mathrm{T}'(\Sigma, \Pi)$. Given an arbitrary solution f for (Σ', Π'), let $\mathbf{R}(f)$ be the set of regions $R \equiv (\sigma, \eta)$ in T' such that $f(x_k) = |\eta|(\mathrm{x}_k^*)$ for all $k \in \{0, \dots, N\}$ and $f(x^\alpha) = |\eta|(\mathrm{x}_*^\alpha)$ for all $\alpha \in A$. Finally let A_* be a disjoint copy of A and let $\cdot_*$ be a bijective mapping from A onto A_*.

Definition 37 (*Type of a region*). The *type* of region $R \equiv (\sigma, \eta) \in \mathbf{R}(f)$ is the map $\tau : A \cup B \cup [0, n-1] \cup A_* \to \{0, 1\}$ given by

$$\tau(\alpha) = \sigma(\mathrm{s}_0^\alpha) \qquad \tau(\beta) = \sigma(\mathrm{t}_0^\beta) \qquad \tau(k) = 0 \Leftrightarrow \eta(\mathrm{x}_k^*) \geqslant 0 \qquad \tau(\alpha_*) = \sigma(\mathrm{w}_3^\alpha)$$

for $\alpha \in A$, $\beta \in B$, $k \in [0, n-1]$, and $\alpha_* \in A_*$.

Definition 38 (*Dependent type of a region*). The *dependent type* of region $R \equiv (\sigma, \eta) \in \mathbf{R}(f)$ is the induced restriction of the map η on the set $YZ = \cup\{\{\mathrm{y}_k^\gamma, \mathrm{z}_k^\gamma\} \mid k \in [0, \dots, N] \wedge \gamma \in \Gamma(k)\}$.

Proposition 39. *Let f be a fixed solution for (Σ', Π'). A region $R \equiv (\sigma, \eta) \in \mathbf{R}(f)$ is totally determined from its type, its dependent type, its value $\sigma(w_0^\alpha)$ at the initial state of each component W_L^α, and its value $\sigma(u_k^\gamma)$ at one initial state in each component UV_k. Conversely, every map $\tau : A \cup B \cup A_* \cup [0, n-1] \to \{0, 1\}$ types a non empty set of regions $(\sigma, \eta) \in \mathbf{R}(f)$ and determines uniquely the common restriction η_τ of their η-component on $E \backslash YZ$ (where E is the set of events of T' and YZ is the set introduced in the above definition). Moreover, $|\eta_\tau(x_k^*)| = |\eta_\tau(x_k^\gamma)|$ for every $k \in [0, \dots, N]$ and $\gamma \in \Gamma(k)$, and a map $\delta : YZ \to \{-1, 0, 1\}$ is the dependent type of a region of type τ if and only if the following are satisfied for all k and γ:*

1. $\eta_\tau(x_k^*) = \eta_\tau(x_k^\gamma) = 0 \quad \Rightarrow \delta(y_k^\gamma) + \delta(z_k^\gamma) = 0$
2. $\eta_\tau(x_k^*) = \eta_\tau(x_k^\gamma) \neq 0 \quad \Rightarrow \delta(y_k^\gamma) = \delta(z_k^\gamma) = 0$
3. $\eta_\tau(x_k^*) = -\eta_\tau(x_k^\gamma) \neq 0 \Rightarrow [\delta(y_k^\gamma) = \eta_\tau(x_k^\gamma) \wedge \delta(z_k^\gamma) = 0]$
   $\vee [\delta(y_k^\gamma) = 0 \wedge \delta(z_k^\gamma) = \eta_\tau(x_k^\gamma)]$

Proof. In order to establish the last claim made in the proposition, it suffices to verify that all and only the maps from $\{\mathrm{x}_k^*, \mathrm{x}_k^\gamma, \mathrm{y}_k^\gamma, \mathrm{z}_k^\gamma\}$ to $\{-1, 0, 1\}$ that coincide with signed regions in UV_k^γ appear as entries in Table 2. Once this verification has been done, one may delete temporarily all components UV_k and focus on regions (σ, η) in $T' \setminus \bigcup_k UV_k$ subject to the constraints $\rho(\mathrm{x}_k^\gamma) = \rho(\mathrm{x}_k^*)(= f(x_k))$ imposed by the omitted components (where $\rho = |\eta|$ is the induced abstract region). One may also delete temporarily all components W_L^α, imposing constraints $\rho(\mathrm{x}_0^*) \cdot \rho(\mathrm{x}_*^\alpha) = 0$ automatically satisfied by assumption on f as soon as $f(x^\alpha) = \rho(\mathrm{x}_*^\alpha)$. We are left with a transition system $T'' = T' \setminus ((\bigcup_k UV_k) \cup (\bigcup_\alpha W_l^\alpha))$ with the unique occurrence property, meaning that each event has at most one occurrence.

The events which occur in T'' may have the form x_k^α, x_k^β, or x_l^* where $\alpha \in A$, $0 \leqslant k \leqslant N$, $\beta \in B$, and $n < l < N$. In particular, all events x_k^* with $k < n$ have disappeared (since $n \leqslant \alpha_j$ for $j \leqslant 3$). By the unique occurrence property and because f is a solution of (Σ', Π'), every subset of $\{\mathrm{s}_0^\alpha \mid \alpha \in A\} \cup \{\mathrm{t}_0^\beta \mid \beta \in B\} \cup \{\mathrm{w}_0^\alpha \mid \alpha \in A\}$ determines a unique region (σ, η) in T'', such that $\rho(\mathrm{x}_k^\alpha) = f(x_k)$, $\rho(\mathrm{x}_k^\beta) = f(x_k)$, $\rho(\mathrm{x}_l^*) = f(x_l)$, and $\rho(\mathrm{x}_*^\alpha) = f(x^\alpha)$, for $\alpha \in A$, $0 \leqslant k \leqslant N$, $\beta \in B$, and $n < l < N$. The

Table 2

x_k^*	x_k^γ	y_k^γ	z_k^γ
0	0	0	0
0	0	1	−1
0	0	−1	1
1	1	0	0
−1	−1	0	0
1	−1	-1	0
−1	1	1	0
1	−1	0	−1
−1	1	0	1

choice for σ is encoded bijectively by the map $\tau : A \cup B \cup A^* \to \{0,1\}$ given by $\tau(\alpha) = \sigma\ (s_0^\alpha)$, $\tau(\beta) = \sigma\ (t_0^\beta)$, and $\tau(\alpha_*) = \sigma\ (w_*^\alpha)$.

Observe by the way that $\eta(x_*^\alpha)$ has been fixed by the above process. In order to extend η into a signed region of T', it remains to fix $\eta(x_k^*)$ for all $k < n$, and subsequently to fix $\eta(y_k^\gamma)$ and $\eta(z_k^\gamma)$ for all $0 \leqslant k \leqslant N$, and $\gamma \in \Gamma\ (k)$. By the first part of this proof, every map $\tau : [0, n-1] \to \{0,1\}$ given jointly with a map $\delta\ : YZ \to \{-1,0,1\}$, compatible with the extended map $\tau : A \cup B \cup A^* \cup [0, n-1] \to \{0,1\}$, defines uniquely a signed region of type τ and dependent type δ in T'.

In order to get a fully defined region (σ, η) in T', it remains to extend σ on all components UV_k and W_L^α. For each component $G = UV_k$ or $G = W_L^\alpha$, two situations can occur. In case when $\eta\ (e) \neq 0$ for some event e occurring in G, the map η determines uniquely the map σ at all states in G since G is connected. In case when $\eta\ (e) = 0$ for all event e occurring in G, the map σ has a constant value on G which may be chosen freely in the set $\{0,1\}$. The value of σ on G is then entirely fixed from the data of $\sigma\ (u_k)$ if $G = UV_k$ or $\sigma\ (w_0^\alpha)$ if $G = W_L^\alpha$. $\square$

Armed with this proposition, and assuming a distinguished solution f_0 for (Σ', Π'), we now start to prove that all instances of ESSP can be solved in T'. Once this result has been established, one verifies easily that all instances of SSP can be solved: most pairs of distinct states (s_1, s_2) in T' are split by some event e, enabled at s_1 and disabled at s_2 (or the converse), and SSP is then automatically solved at (s_1, s_2) when ESSP is solved at (s_2, e). The pairs of states which remain to be checked for separation are all pairs of sink states, plus the pairs (u_0, w_1^α), (w_2^α, w_6^α), $(u_{\alpha_j}, w_j^\alpha)$, and $(\mathcal{U}_k^\gamma, \mathcal{V}_k^\gamma)$, where $\alpha \in A, j \in \{3,4,5\}, k \in [0, N]$ and $\gamma \in \Gamma(k)$. If we except pairs $(\mathcal{U}_k^\gamma, \mathcal{V}_k^\gamma)$, all these pairs are assembled from states in two different connected components of T', and their separation makes no problem since the set of states of a connected component is always a region. For the remaining pairs $(\mathcal{U}_k^\gamma, \mathcal{V}_k^\gamma)$, separation follows from Proposition 39 applied to any solution f of (Σ', Π') such that $f(x_k) = 1$ (where $\tau(\gamma)$ is chosen so that $\eta_\tau(x_k^*) = \eta_\tau(x_k^\gamma)$).

In order to divide the proof into meaningful pieces, let us introduce one more definition.

Definition 40. For any pair (G_1, G_2) of connected components of T', let $G_1 \lhd G_2$ if there exists in T' a region which inhibits e at s for every event e occurring in G_1 and for every state s in G_2 such that e is disabled at s.

In order to establish Theorem 26 it remains to prove that $G_1 \lhd G_2$ for every pair of connected components (G_1, G_2), where possibly $G_1 = G_2$. This will be proved by a series of lemmas, given in the remaining part of the paper. On several occasions, we shall use the following fact about regions, which was observed in [2] and can easily be verified by the reader.

Fact 41. *The union of* disjoint *regions is a region. If R_1 and R_2 are regions with $R_1 \subset R_2$, then $R_2 \backslash R_1$ is a region.*

Lemma 42. *$G \lhd G'$ for $G \in \{S^\alpha, T^\beta, W_L^\alpha, W_R^\alpha\}$ and $G' \in \{S^{\alpha'}, T^{\beta'}, W_L^{\alpha'}, W_R^{\alpha'}\}$, where $\alpha \neq \alpha'$ and $\beta \neq \beta'$.*

Proof. An event e occurring in G may have the form x_k^α or x_k^β for $k \leqslant N$, or x_*^α, or x_0^*, or x_k^* for $k \geqslant n$ (viz. $k = \alpha_j$ and $j \geqslant 3$). According to the case, let $x' \in X'$ be the variable x_k, x^α or x_0 then $f(x') = 1$ for some solution f of (Σ', Π'). From Proposition 39 applied to f, one may construct a region $R \equiv (\sigma, \eta) \in \mathbf{R}(f)$ such that $\eta(e) = -1$ with an adequate choice for $\tau(\alpha)$, $\tau(\beta)$, $\tau(\alpha_*)$, or $\tau(0)$ according to the form of e. If $\eta(e') = 0$ for every e' occurring in G', then the region $R' = (R \backslash G')$ inhibits e at every state s' in G'. Let us examine the converse case. If $G' \in \{S^{\alpha'}, T^{\beta'}, W_R^{\alpha'}\}$, let τ' be defined like τ except at α', β', or α'_* according to the form of G'. From Proposition 39, there exists a region $R' \equiv (\sigma', \eta') \in \mathbf{R}(f)$ with type τ'. Now the maps σ and σ' take complementary values at every state in G', hence for each state s' in G' either R or R' inhibits e at s'. Finally let $G' = W_L^{\alpha'}$. If $e = x_0$, R inhibits e at w_2^α and w_7^α. In the converse case, let τ' be defined like τ except at 0 if $\eta(\mathrm{x}_0^*) \neq 0$ or at α'_* if $\eta(\mathrm{x}_*^{\alpha'}) \neq 0$. From Proposition 39, there exists a region $R' \equiv (\sigma', \eta') \in \mathbf{R}(f)$ with type τ'. The maps σ and σ' take complementary values on G', and the conclusion follows as above. $\square$

Fact 43. $S^\alpha \lhd W_L^\alpha$, $S^\alpha \lhd W_R^\alpha$, $W_L^\alpha \lhd S^\alpha$, *and* $W_R^\alpha \lhd S^\alpha$.

Lemma 44. $W_L^\alpha \lhd W_L^\alpha$, $W_L^\alpha \lhd W_R^\alpha$, $W_R^\alpha \lhd W_L^\alpha$, *and* $W_R^\alpha \lhd W_R^\alpha$.

Proof. An event e occurring in W^α may have form x_0^*, or x_k^* for $k \geqslant n$, or x_*^α. Let us examine separately the three cases.

If $e = \mathrm{x}_0^*$, one applies Proposition 39 to the distinguished solution f_0 of (Σ', Π'), providing for a suitable choice of $\tau(0)$ a region $R \equiv (\sigma, \eta) \in \mathbf{R}(f_0)$ such that $\eta(\mathrm{x}_0^*) = -1$, and $\eta(e') = 0$ for every e' occurring in W_R^α. Now by Fact 41, the region $R \backslash W_R^\alpha$ inhibits x_0^* wherever it is not enabled in W^α.

If $e = \mathrm{x}_k^*$ and $k = \alpha_j$ $(j \geqslant 3)$, consider the solution f of (Σ', Π') defined by $f(x_h) = 1$ for $h \in \{\alpha_j, \alpha_{3+(j-1) \bmod 3}\}$ and $f(x') = 0$ for all the other variables. From

Proposition 39 applied to f with a suitable choice for $\tau(\alpha_*)$, one constructs a region $R \equiv (\sigma,\eta) \in \mathbf{R}(f)$ such that $\eta(e) = -1$. We proceed by case analysis according to the value of j. If $j = 4$ or $j = 5$, the region $R \setminus W_L^{\alpha}$ inhibits e at every state s where it is not enabled in W^{α}. If $j = 3$, the same holds except for state w_6^{α}. In order to deal with this exception, we construct another solution f' for (Σ',Π'), such that $f'(x^{\alpha}) = f'(x_{\alpha_3}) = 1$. For that purpose, choose $i \in \{0,1,2\}$ such that $\alpha_i \neq 0$ and let $h = \alpha_i$. Then set $f'(x_h) = 1$, $f'(x^{\gamma}) = 1$ and $f'(x_{\gamma_3}) = 1$ iff $h \in \{\gamma_0,\gamma_1,\gamma_2\}$, and $f'(x') = 0$ for all the other variables. From Proposition 39 applied to f' for a suitable choice for $\tau(\alpha_*)$, one obtains a region $R' \equiv (\sigma',\eta') \in \mathbf{R}(f')$ such that $\eta(e) = -1$, and R' inhibits e at state w_6^{α}.

If $e = \mathrm{x}_*^{\alpha}$, we construct in a similar way a solution f' for (Σ',Π') such that $f'(x^{\alpha}) = f'(x_{\alpha_5}) = 1$ and $f'(x_{\alpha_3}) = f'(x_{\alpha_4}) = 0$. We obtain therefrom a region $R' \equiv (\sigma',\eta') \in \mathbf{R}(f')$ such that $\eta'(e) = -1$, and R' inhibits e wherever it is not enabled in W^{α}. □

Fact 45. *Let f be a solution for (Σ',Π'), then for each $\alpha \in A$, $i \in \{0,1,2\}$ and $j \in \{1,2\}$, the function f' defined by $f'(x_{\alpha_k}) = 1 + f(x_{\alpha_k})$ if $k \in \{3+i, 3+(i+j) \bmod 3\}$, and $f'(x) = f(x)$ for all the other variables in X', is also a solution for (Σ',Π').*

Lemma 46. $S^{\alpha} \lhd S^{\alpha}$.

Proof. Let $e = \mathrm{x}_k^{\alpha}$ and $k = \alpha_i$. We examine separately the cases $i \leqslant 2$ and $i \geqslant 3$.

If $i \leqslant 2$, let f be a solution of (Σ',Π') such that $f(x_k) = 1$. From Fact 45, there exists another solution f' such that $f'(x_{\alpha_j}) = 1 + f(x_{\alpha_j})$ for $j \in \{3+i, 3+(i+2) \bmod 3\}$, and $f'(x') = f(x')$ for all the other variables in X'. From Proposition 39, applied to f and f' with a suitable choice for $\tau(\alpha)$, one may construct respective regions $R \equiv (\sigma,\eta) \in \mathbf{R}(f)$ and $R' \equiv (\sigma',\eta') \in \mathbf{R}(f')$ such that $\eta(e) = \eta'(e) = -1$, whence for every state $s \neq \mathrm{s}_i^{\alpha}$ either R or R' inhibits e at s in S^{α}.

If $i \geqslant 3$, we set $j = i-3$ and $h = \alpha_j$, and we proceed separately for cases $h \neq 0$ and $h = 0$.

If $h \neq 0$, consider the solution f of (Σ',Π') defined by $f(x_h) = 1$, $f(x^{\gamma}) = 1$ for $\gamma \in A$ iff $h = \gamma_l$ for some l ($\leqslant 2$), $f(x_{\gamma_{l+3}}) = 1$ for such γ and l, and $f(x') = 0$ for all the other variables in X'. From Proposition 39 applied to f with a suitable choice for $\tau(\alpha)$, one obtains a region $R \equiv (\sigma,\eta) \in \mathbf{R}(f)$ such that $\eta(e) = -1$, and R inhibits e in S^{α} at every state $s \neq \mathrm{s}_i^{\alpha}$.

If $h = 0$, consider the distinguished solution f_0 of (Σ',Π'). Let l be the (unique) integer in $\{0,1,2\}$ such that $l \neq j$ and $f_0(x_{\alpha_l}) = 1$. One derives from f_0 another solution f for (Σ',Π') by setting $f(x_{\alpha_l}) = f(x_{\alpha_{l+3}}) = 1$ and $f(x') = f_0(x')$ for all the other variables in X'. From Proposition 39 applied to f with a suitable choice for $\tau(\alpha)$, one obtains a region $R \equiv (\sigma,\eta) \in \mathbf{R}(f)$ such that $\eta(e) = -1$, and R inhibits e in S^{α} at all states $s \neq \mathrm{s}_i^{\alpha}$ except at state $\mathrm{s}_{l+3}^{\alpha}$. In order to cope with this exception, consider the solution f' of (Σ',Π') defined by $f'(x_{\alpha_l}) = f'(x_{\alpha_{l+3}}) = 1$ and $f'(x') = 0$ for all the other variables in X'. From Proposition 39 applied to f' with a suitable choice for $\tau(\alpha)$, one obtains a region $R' \equiv (\sigma', \eta') \in \mathbf{R}(f')$ such that $\eta'(e) = -1$, and R' inhibits e at state $\mathrm{s}^{\alpha}_{l+3}$. $\square$

Fact 47 (by Fact 29). $T^{\beta} \lhd T^{\beta}$.

Lemma 48. *$G \lhd UV_k$ for $G \in \{S^{\alpha}, T^{\beta}, W^{\alpha}_{L}, W^{\alpha}_{R}\}$.*

Proof. Let e be an event occurring in G. Let $x = x_h$ if $e = \mathrm{x}^{\alpha}_{h}$ or $e = \mathrm{x}^{\beta}_{h}$ or $e = \mathrm{x}^{*}_{h}$, and let $x = x^{\alpha}$ if $e = \mathrm{x}^{\alpha}_{*}$. We proceed separately with cases $x \notin \{x_0, x_k\}$, $x = x_k$, and $x = x_0$.

Suppose $x \notin \{x_0, x_k\}$. From Facts 29 and 30, there exists in that case a solution f for (Σ', Π') such that $f(x) = 1$ and $f(x_k) = 0$. From Proposition 39, applied to f with a suitable choice for $\tau(\alpha)$ (if $G = S^{\alpha}$) or $\tau(\beta)$ (if $G = T^{\beta}$) or $\tau(\alpha_*)$ (if $G = W^{\alpha}_{L}$ or $G = W^{\alpha}_{R}$), one may construct a region $R \equiv (\sigma, \eta) \in \mathbf{R}(f)$ such that $\eta(e) = -1$ and $\eta(\mathrm{y}^{\gamma}_{k}) = \eta(\mathrm{z}^{\gamma}_{k}) = 0$ for all $\gamma \in \Gamma(k)$. Now by Fact 41, $R \backslash UV_k$ is a region which inhibits e at all states in UV_k.

Suppose $x = x_k$ then either $k < n$ or $k = \alpha_j$ for some $\alpha \in A$ and $j \geqslant 3$. In either case, let f be a solution for (Σ', Π') such that $f(x) = 1$. If $e = \mathrm{x}^{*}_{k}$, one obtains from Proposition 39, applied to f with the suitable choice for $\tau(k)$ (if $k < n$ i.e. if $k = 0$) or $\tau(\alpha_*)$ and all possible choices for $\{\tau(\gamma) \mid \gamma \in \Gamma(k)\}$, a family of regions $R_i \equiv (\sigma_i, \eta_i) \in \mathbf{R}(f)$ such that $\eta_i(e) = -1$ and every map $\eta : \{\mathrm{x}^{\gamma}_{k} \mid \gamma \in \Gamma(k)\} \to \{-1, 1\}$ coincides with the restriction of some signed region η_i. If $e = \mathrm{x}^{\delta}_{k}$ for some $\delta \in \Gamma(k)$, one obtains from Proposition 39, applied to f with the suitable choice for $\tau(\delta)$ and with all possible choices for $\{\tau(\gamma) \mid \gamma \neq \delta \wedge \gamma \in \Gamma(k)\}$ and $\tau(k)$ (if $k < n$) or $\tau(\alpha_*)$, a family of regions $R_i \equiv (\sigma_i, \eta_i) \in \mathbf{R}(f)$ such that $\eta_i(e) = -1$ and every map $\eta : \{\mathrm{x}^{*}_{k}\} \cup \{\mathrm{x}^{\gamma}_{k} \mid \gamma \neq \delta \wedge \gamma \in \Gamma(k)\} \to \{-1, 1\}$ coincides with the restriction of some signed region η_i. In both situations, some region R_i in the resulting set inhibits e at each state u_k, v_k, u^{γ}_{k}, or v^{γ}_{k} in which it is not enabled. By varying now the dependent type of each region R_i according to the conditions stated in Proposition 39 (with η_i substituted for η_τ and δ), one obtains additional regions which inhibit e at all the remaining states $\mathscr{U}^{\gamma}_{k}$ and $\mathscr{V}^{\gamma}_{k}$.

Suppose finally $x = x_0$ and $k \neq 0$. Consider the distinguished solution f_0 of (Σ', Π'). If $f_0(x_k) = 0$, which is always true for $k \geqslant n$, one obtains from Proposition 39, applied to f_0 with a suitable choice for $\tau(\alpha)$ (if $e = \mathrm{x}^{\alpha}_{0}$) or $\tau(0)$ (if $e = \mathrm{x}^{*}_{0}$),[4] a region $R \equiv (\sigma, \eta) \in \mathbf{R}(f_0)$ such that $\eta(e) = -1$, $\eta(\mathrm{x}^{*}_{k}) = 0$ and $\eta(\mathrm{x}^{\gamma}_{k}) = 0$ for all $\gamma \in \Gamma(k)$. From Proposition 39, the dependent type of R may be adjusted so that $\eta(\mathrm{y}^{\gamma}_{k}) = \eta(\mathrm{z}^{\gamma}_{k}) = 0$ for all $\gamma \in \Gamma(k)$. Now by Fact 41, $R \backslash UV_k$ is a region which inhibits e at all states in UV_k. If $f_0(x_k) = 1$ (thus $0 < k < n$), we proceed separately for the case $e = \mathrm{x}^{\alpha}_{0} \wedge \alpha \in \Gamma(k)$ and for the other cases.

[4] Remember that variable x_0 does not occur in equations Π thus there is no event of the form x^{β}_{0} for $\beta \in B$.

Let $e = \mathrm{x}_0^*$, or $e = \mathrm{x}_0^\alpha$ and $\alpha \notin \Gamma(k)$. From Proposition 39, applied to f_0 with a suitable choice for $\tau(0)$ or $\tau(\beta)$ or $\tau(\alpha)$, and with all possible choices for $\{\tau(\gamma) \mid \gamma \in \Gamma(k)\}$, one obtains a family of regions $R_i \equiv (\sigma_i, \eta_i) \in \mathbf{R}(f_0)$ such that $\eta_i(e) = -1$ and every map $\eta : \{\mathrm{x}_k^\gamma \mid \gamma \in \Gamma(k)\} \to \{-1, 1\}$ coincides with the restriction of some signed region η_i. The expected conclusion follows like in case $x = x_k$.

Let finally $e = \mathrm{x}_0^\alpha$ and $\alpha \in \Gamma(k)$, whence $0 = \alpha_i$ and $k = \alpha_j$ for two distinct integers $i, j \in \{0, 1, 2\}$. Since f_0 is a distinguished solution of (Σ', Π'), $f_0(x_{\alpha_p}) = 0$ for all $p \in [0, 5] \setminus \{i, j\}$. From Fact 45, there exists another solution f for (Σ', Π') such that $f(x_{\alpha_p}) = 1$ for $p \in \{3 + j, 3 + (j + 2) \bmod 3\}$, and $f(x') = f_0(x')$ for all the other variables in X'. From Proposition 39, applied to f with a suitable choice for $\tau(\alpha)$, and with all possible choices for $\tau(k)$ and for $\{\tau(\gamma) \mid \gamma \neq \alpha \wedge \gamma \in \Gamma(k)\}$, one obtains a family of regions $R_i \equiv (\sigma_i, \eta_i) \in \mathbf{R}(f)$ such that $\eta_i(e) = -1$ and every map $\eta : \{\mathrm{x}_k^*\} \cup \{\mathrm{x}_k^\gamma \mid \gamma \neq \alpha \wedge \gamma \in \Gamma(k)\} \to \{-1, 1\}$ coincides with the restriction of some signed region η_i. The expected conclusion follows again like in case $x = x_k$. $\square$

Fact 49. *For all k and $\gamma \in \Gamma(k)$, the sets $\{\mathscr{U}_k^\gamma, \mathscr{V}_k^\gamma\}$ and $UV_k \setminus \{\mathscr{U}_k^\gamma, \mathscr{V}_k^\gamma\}$ define respective regions $R \equiv (\sigma, \eta)$ and $R' \equiv (\sigma', \eta')$ in T' such that $\eta(z_k^\gamma) = -1$ and $\eta'(y_k^\gamma) = -1$. Similarly, the set $\cup\{\{\mathscr{U}_k^\gamma, \mathscr{V}_k^\gamma\} \mid \gamma \in \Gamma(k)\}$ and its complement in UV_k are regions.*

Lemma 50. *$UV_k \lhd UV_l$ for $k \neq l$.*

Proof. In view of Fact 49, it suffices to show that ESSP may be solved at all instances (e, s) in which s is a state in UV_l and $e = \mathrm{x}_k^*$ or $e = \mathrm{x}_k^\beta$ or $e = \mathrm{x}_k^\alpha$. Now in every case except when $e = \mathrm{x}_k^*$ and $0 < k < n$, ESSP may be solved at (e, s) as a consequence from $S^\alpha \lhd UV_l$, or $T^\beta \lhd UV_l$, or $W_L^\alpha \lhd UV_l$, or $W_R^\alpha \lhd UV_l$. So assume $e = \mathrm{x}_k^*$ and $0 < k < n$. There exists a solution f for (Σ', Π') such that $f(x_k) = 1$ and $f(x_l) = 0$. From Proposition 39, applied to f with a suitable choice for $\tau(k)$, there exists a region $R \equiv (\sigma, \eta) \in \mathbf{R}(f)$ such that $\eta(e) = -1$ and $\eta(e') = 0$ for every e' in UV_l. Then $R \setminus UV_l$ is a region that inhibits e everywhere in UV_l. $\square$

Lemma 51. *$UV_k \lhd UV_k$.*

Proof. In view of the properties $S^\alpha \lhd UV_k$, $T^\beta \lhd UV_k$, $W_L^\alpha \lhd UV_k$, and $W_R^\alpha \lhd UV_k$, it suffices to solve ESSP at (e, s) for s in UV_k and $e = \mathrm{z}_k^\gamma$, or $e = \mathrm{y}_k^\gamma$, or $e = \mathrm{x}_k^*$ and $0 < k < n$. The first case is immediate (from Fact 49). We examine separately the remaining cases.

Suppose $e = \mathrm{x}_k^*$ (with $0 < k < n$). Let then f be a solution for (Σ', Π') such that $f(x_k) = 1$. From Proposition 39, applied to f with the suitable choice for $\tau(k)$ and with all possible choices for $\{\tau(\gamma) \mid \gamma \in \Gamma(k)\}$, one obtains a family of regions $R_i \equiv (\sigma_i, \eta_i) \in \mathbf{R}(f)$ such that $\eta_i(e) = -1$ and every map $\eta : \{\mathrm{x}_k^\gamma \mid \gamma \in \Gamma(k)\} \to \{-1, 1\}$ coincides with the restriction of some signed region η_i. As a consequence, some region in the family inhibits e at each state u_k, v_k, u_k^γ, or v_k^γ in which it is not enabled. By varying the dependent type of each region R_i according to the conditions stated in Proposition 39 (with η_i substituted for η_τ and δ), one obtains additional regions which inhibit e at all the remaining states $\mathscr{U}_k^\gamma$ and $\mathscr{V}_k^\gamma$.

Suppose now $e = y_k^\gamma$, where either $k < n$ or $k = \alpha_j$ ($j \geqslant 3$). Since the set $\cup\{\{\mathscr{U}_k^\delta, \mathscr{V}_k^\delta\} \mid \delta \in \Gamma(k)\}$ and its complement in UV_k are regions, it suffices in fact to solve ESSP at (e,s) for $s = u_k$ or v_k^γ, and for $s = u_k^\delta$ or v_k^δ with $\delta \neq \gamma$. Let f be a solution for (Σ', Π') such that $f(x_k) = 1$. From Proposition 39, applied to f with a suitable choice for $\tau(k)$ (if $k < n$) or $\tau(\alpha'_*)$ (if $k \geqslant n$) and for $\{\tau(\delta) \mid \delta \in \Gamma(k)\}$, one may construct a region $R \equiv (\sigma, \eta) \in \mathbf{R}(f)$ such that $\eta(x_k^*) = 1$ and $\eta(x_k^\delta) = -1$ for all $\delta \in \Gamma(k)$ (including γ). From Proposition 39, one may adjust the dependent type of R so that $\eta(y_k^\gamma) = -1$, and then R inhibits e at u_k and at all states v_k^δ ($\delta \in \Gamma(k)$). The converse choice for $\{\tau(\delta) \mid \delta \neq \gamma \wedge \delta \in \Gamma(k)\}$ produces a region $R' \equiv (\sigma', \eta') \in \mathbf{R}(f)$ such that $\eta'(x_k^*) = 1$, $\eta'(x_k^\gamma) = -1$, and $\eta(x_k^\delta) = 1$ for $\delta \neq \gamma$. This region R' inhibits e at all states u_k^δ ($\delta \in \Gamma(k)$ and $\delta \neq \gamma$). □

Lemma 52. *$UV_k \lhd S^\alpha$ and $UV_k \lhd T^\beta$.*

Proof. In view of Fact 49 and properties $S^\gamma \lhd S^\alpha$, $T^\gamma \lhd S^\alpha$, $W_L^\gamma \lhd S^\alpha$, $W_R^\gamma \lhd S^\alpha$, and $S^\gamma \lhd T^\beta$, $T^\gamma \lhd T^\beta$, $W_L^\gamma \lhd T^\beta$, $W_R^\gamma \lhd T^\beta$, it suffices to solve ESSP at (e,s) for s in S^α or T^β and $e = x_k^*$ with $0 < k < n$. Let f be a solution for (Σ', Π') such that $f(x_k) = 1$. From Proposition 39, applied to f with a suitable choice for $\tau(k)$, one may construct a region $R \equiv (\sigma, \eta)$ of type τ in $\mathbf{R}(f)$ such that $\eta(x_k^*) = -1$. Let type τ' be defined like τ except at α (respectively, at β). From Proposition 39, there exists a region $R' \equiv (\sigma', \eta')$ of type τ' in T'. Now the maps σ and σ' take complementary values at each state s in S^α (respectively, T^β), hence at each state s, either R or R' inhibits x_k^*. □

Lemma 53. *$UV_k \lhd W_L^\alpha$ and $UV_k \lhd W_R^\alpha$.*

Proof. For the same reasons as in the preceding lemma, it suffices to solve ESSP at (e,s) for s in W_L^α or W_R^α and $e = x_k^*$ with $0 < k < n$. Let f be a solution for (Σ', Π') such that $f(x_k) = 1$. From Proposition 39, applied to f with a suitable choice for $\tau(k)$, one may construct a region $R \equiv (\sigma, \eta)$ of type τ in $\mathbf{R}(f)$ such that $\eta(x_k^*) = -1$. Let type τ' be definedlike τ except at α_*. From Proposition 39, there exists a region $R' \equiv (\sigma', \eta')$ of type τ' in T'. Now the maps σ and σ' take complementary values at each state s in W_R^α, hence at each state s in W_R^α, either R or R' inhibits x_k^* at state s. This line of reasoning is also valid for W_L^α if $f(x^\alpha) = 1$ (τ' is like τ except at α_*) or $f(x^\alpha) = 0$ and $f(x_0) = 1$ (τ' is defined like τ except at 0). Consider finally the case where $f(x^\alpha) = f(x_0) = 0$. Then $R \setminus W_L^\alpha$ is a region which inhibits x_k^* at all states in W_L^α. □

The above series of lemmas show that $G_1 \lhd G_2$ for every pair of connected components (G_1, G_2) in T', as required, hence the proof for Theorem 26 is complete.

References

[1] E. Badouel, L. Bernardinello and Ph. Darondeau, Polynomial algorithms for the synthesis of bounded nets, *Proc. CAAP'95*, Lectures Notes in Computer Science, Vol. 915 (Springer, Berlin, 1995) 364–378.

[2] L. Bernardinello, Synthesis of net systems, *Proc. ICATPN'93*, Lectures Notes in Computer Science, Vol. 691 (Springer, Berlin, 1993) 89–105.

[3] L. Bernardinello, G. De Michelis, K. Petruni and S. Vigna, On the synchronic structure of transition systems, in: J. Desel, ed., *Structures in Concurrency Theory (STRICT)* (Springer, Berlin, 1996) 11–13.

[4] J. Cortadella,, M. Kishinevsky, A. Kondratyev, L. Lavagno and A. Yakovlev, Complete State Encoding based on the Theory of Regions, *Proc. 2nd Internat. Symp. on Advanced Research in Asynchronous Circuits and Systems* (IEEE Computer Society Press, Silver Spring, MD, 1996).

[5] J. Cortadella, M. Kishinevsky, L. Lavagno and A. Yakovlev, Synthesizing Petri nets from state-based models, *Proc. ICCAD'95* (IEEE Computer Society Press, Silver Spring, MD, 1995) 164–171.

[6] J. Desel and W. Reisig, The synthesis problem of Petri nets, *Acta Informatica* **33** (1996) 297–315.

[7] M. Droste and R.M. Shortt, Petri nets and automata with concurrency relations – an adjunction, in: M. Droste and Y. Gurevich, eds., *Semantics of Programming Languages and Model Theory* (Gordon and Breach, 1993) 69–87.

[8] A. Ehrenfeucht and G. Rozenberg, Partial 2-structures; Part I: Basic notions and the representation problem, and Part II: State spaces of concurrent systems, *Acta Inform.* **27** (1990) 315–368.

[9] M.R. Garey and D.S. Johnson, *Computer and Intractability. A Guide to the theory of* NP-*Completeness*. (Freeman, New York, 1979).

[10] M. Gondran and M. Minoux, *Graphes et Algorithmes* (Eyrolles, Paris, 1985).

[11] K. Hiraishi, Some complexity results on transitions systems and elementary net systems, *Theoret. Comput. Sci.* **135** (1994) 361–376.

[12] M. Mukund, Petri nets and step transition systems, *Internat. J. Foundation Comput. Sci.* **3**(4) (1992) 443–478.

[13] V. Schmitt, Flip-flop nets, *Proc. STACS'96*, Lectures Notes in Computer Science, Vol. 1046 (Springer, Berlin, 1996) 517–528.